

NETGEAR®

CLI Command Reference Manual

Fully Managed Switches M4250 and M4350 Series

M4250: Firmware version 13.0.0 and later versions

M4350: Firmware version 14.0.0 and later versions

April 2026
202-12843-04

NETGEAR, Inc.
3553 N First Street,
San Jose, CA 95134, USA

Support and Community

Visit [netgear.com/support](https://www.netgear.com/support) to get your questions answered and access the latest downloads.

You can also check out our NETGEAR Community for helpful advice at community.netgear.com.

Regulatory and Legal

Si ce produit est vendu au Canada, vous pouvez accéder à ce document en français canadien à <https://www.netgear.com/support/download/>.

(If this product is sold in Canada, you can access this document in Canadian French at <https://www.netgear.com/support/download/>.)

For regulatory compliance information including the EU Declaration of Conformity, visit <https://www.netgear.com/about/regulatory/>.

See the regulatory compliance document before connecting the power supply.

For NETGEAR's Privacy Policy, visit <https://www.netgear.com/about/privacy-policy>.

Where permitted by law, by using this device, you are agreeing to NETGEAR's Terms and Conditions at <https://www.netgear.com/about/terms-and-conditions>. If you do not agree, return the device to your place of purchase within your return period.

This product is designed and warranted for indoor use only. Do not use this device outdoors. The PoE source is intended for intra building connection only.

Trademarks

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

Revision History

Publication Part Number	Publish Date	Comments
202-12843-04	April 2026	Updated the default bridge-aging timeout in MAC Database Commands, Chapter 7, Switching Commands . We added the Expandable Port Configurations in Chapter 7 section.
202-12843-03	November 2025	We added the following commands to Chapter 7, Switching Commands : • <code>rgb-led mode</code> • <code>rgb-led color</code> • <code>show rgb-led color configuration</code> • <code>show rgb-led color configuration all</code>
202-12843-02	July 2025	We added the following commands to Chapter 7, Switching Commands : • <code>vlan association oui</code> • <code>show vlan association oui</code> • <code>ptp ieee version 2.0</code>
202-12843-01	February 2025	Initial publication of this manual for both the M4250 series and M4350 series.

Contents

Chapter 1 Introduction and Documentation

Chapter 2 How to Use the Command-Line Interface

Command syntax	10
Command conventions	11
Common parameter values	11
The slot/port (M4250) or unit/slot/port (M4350) naming convention	12
'no' form of a command	14
'show' commands	14
CLI output filtering	14
Command completion and abbreviation	15
CLI error messages	16
CLI line-editing conventions	16
Use the CLI help	17
Access the CLI	18

Chapter 3 CLI Organization and Command Modes

CLI command modes	20
How to enter or exit a command mode	23

Chapter 4 Stacking Commands

Dedicated Port Stacking Commands	29
Stack Port Commands	43
Stack Firmware Synchronization and Copy Commands	49
Nonstop Forwarding Commands for Stack Configuration	52

Chapter 5 Management Commands

Configure the Switch Management CPU	58
CPU Queue Commands	62
Management Interface Commands	63
IPv6 Management Commands	70
Console Port Access Commands	76
Telnet Commands	79
Secure Shell Commands	85
Management Security Commands	94
Management Access Control List Commands	105
Hypertext Transfer Protocol Commands	110
Access Commands	120

User Account Commands	122
Per-Command Authorization	128
Exec Authorization	128
SNMP Commands	162
RADIUS Commands	183
TACACS+ Commands	217
Configuration Scripting Commands	223
Prelogin Banner, System Prompt, and Host Name Commands	226
Application Commands	228
OpenFlow Commands	231
Cloud Managed Commands	243

Chapter 6 Utility Commands

AutoInstall Commands	249
CLI Output Filtering Commands	253
Dual Image Commands	256
System Information and Statistics Commands	258
Switch Services Commands	295
Logging Commands	297
Email Alerting and Mail Server Commands	307
Firmware and File Management Commands	315
System Utility and Clear Commands	320
Network Time Protocol Commands	333
Time Zone Commands	345
DHCP Server Commands	349
DNS Client Commands	371
IP Address Conflict Commands	378
Serviceability Packet Tracing Commands	379
Cable Test Command	426
Power Management Commands	427
USB commands	429
sFlow Commands	432
Switch Database Management Template Commands	441
Green Ethernet Commands	444
Remote Monitoring Commands	453
Statistics Application Commands	470

Chapter 7 Switching Commands

Port Configuration Commands	481
Port Link Flap Commands	492
Spanning Tree Protocol Commands	494
Loop Protection Commands	534
VLAN Commands	538
Switch Port Commands	556
Double VLAN Commands	561
Private VLAN Commands	564

Fully Managed Switches M4250 and M4350 Series

Voice VLAN Commands	567
Precision Time Protocol Commands	571
Provisioning (IEEE 802.1p) Commands	601
Asymmetric Flow Control Commands	601
Protected Port Commands	603
Private Group Commands	606
GARP Commands	608
GVRP Commands	610
GMRP Commands	612
Port-Based Network Access Control Commands	615
Storm-Control Commands	650
Link Dependency Commands	660
Link Local Protocol Filtering Commands	664
Port-Channel/LAG (802.3ad) Commands	665
Port Mirroring Commands	693
ERSPAN Source Switch Configuration Commands	698
Static MAC Filtering Commands	704
DHCP L2 Relay Agent Commands	708
DHCP Client Commands	716
DHCP Snooping Configuration Commands	717
Dynamic ARP Inspection Commands	729
ARP Guard Commands	739
MVR Commands	746
IGMP Snooping Configuration Commands	754
IGMP Snooping Querier Commands	772
MLD Snooping Commands	778
MLD Snooping Querier Commands	792
Port Security Commands	798
LLDP (802.1AB) Commands	806
LLDP-MED Commands	819
Denial of Service Commands	828
MAC Database Commands	841
ISDP Commands	844
Interface Error Disabling and Auto Recovery Commands	853
UniDirectional Link Detection Commands	856
IPv4 Device Tracking Commands	860
Link Debounce Commands	869
Bonjour Commands	870
Audio Video Bridging Commands	872
802.1AS Commands	873
MRP Commands	883
MMRP Commands	885
MVRP Commands	890
MSRP Commands	896

Chapter 8 Routing Commands

Address Resolution Protocol Commands	906
IP Routing Commands	914

Routing Policy Commands	946
Router Discovery Protocol Commands	958
Virtual LAN Routing Commands	963
Virtual Router Redundancy Protocol Commands	967
Virtual Router Redundancy Protocol version 3 Commands	984
DHCP and BootP Relay Commands	999
IP Helper Commands	1004
Open Shortest Path First commands	1012
General OSPF Commands	1013
OSPF Interface Commands	1036
OSPF Graceful Restart Commands	1043
OSPFv2 Stub Router Commands	1046
OSPF Show Commands	1048
IP Event Dampening Commands	1070
Routing Information Protocol Commands	1072
ICMP Throttling Commands	1081
IP Service Level Agreement Commands	1084
IP SLA Configuration Commands	1089

Chapter 9 Captive Portal Commands

Captive Portal Global Commands	1101
Captive Portal Configuration Commands	1107
Captive Portal Status Commands	1119
Captive Portal Client Connection Commands	1122
Captive Portal Interface Commands	1126
Captive Portal Local User and User Group Commands	1128

Chapter 10 IPv6 Commands

Loopback Interface Commands	1140
IPv6 Routing Commands	1141
IPv6 Policy-Based Routing Commands	1188
OSPFv3 Commands	1197
Global OSPFv3 Commands	1198
OSPFv3 Interface Commands	1216
OSPFv3 Graceful Restart Commands	1222
OSPFv3 Stub Router Commands	1225
OSPFv3 Show Commands	1227
DHCPv6 Commands	1245
DHCPv6 Snooping Configuration Commands	1259

Chapter 11 Quality of Service Commands

Class of Service Commands	1273
Differentiated Services Commands	1285
DiffServ Class Commands	1286
DiffServ Policy Commands	1296
DiffServ Service Commands	1304

DiffServ Show Commands	1306
MAC Access Control List Commands	1313
IP Access Control List Commands	1322
IPv6 Access Control List Commands	1339
Time Range Commands for Time-Based ACLs	1349
Auto-Voice over IP Commands	1352
iSCSI Optimization Commands	1358

Chapter 12 IP Multicast Commands

Multicast Commands	1366
DVMRP Commands	1376
PIM Commands	1381
Internet Group Message Protocol Commands	1401
IGMP Proxy Commands	1411

Chapter 13 IPv6 Multicast Commands

IPv6 Multicast Forwarder	1418
IPv6 PIM Commands	1423
IPv6 MLD Commands	1440
IPv6 MLD-Proxy Commands	1449

Chapter 14 Power over Ethernet Commands

About PoE	1457
PoE Commands	1458

Chapter 15 Switch Software Log Messages

Core	1472
Utilities	1474
Management	1477
Switching	1481
QoS	1488
Routing/IPv6 Routing	1489
Multicast	1491
Technologies	1495
O/S Support	1497

Chapter 16 Command List

1

Introduction and Documentation

This command-line interface (CLI) reference manual is for the Fully Managed Switches M4250 Series and M4350 Series and covers all M4250 and M4350 switch models.

You can download the following guides and manuals for the Fully Managed Switches M4250 Series by visiting netgear.com/support/product/m4250/#docs and for the Fully Managed Switches M4350 Series by visiting netgear.com/support/product/m4350#docs.

- Installation Guide
- Hardware Installation Guide
- Main User Manual
- Audio Video User Manual
- Software Administration Manual (M4250 Series only)
- CLI Command Reference Manual (this manual)

For each individual command in this manual, the supported switch series is stated, using the following color coding:

- Green: **M4250**, the command is supported on the M4250 series switches.
- Blue: **M4350**, the command is supported on the M4350 series switches.

Note: For more information about the topics covered in this manual, visit the support website at netgear.com/support.

Note: Firmware updates with new features and bug fixes are made available from time to time at netgear.com/support/download/. 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.

2

How to Use the Command-Line Interface

The command-line interface (CLI) is a text-based way to manage and monitor the system. You can access the CLI by using a direct serial connection or by using a remote logical connection with telnet or SSH.

This chapter describes the CLI syntax, conventions, and modes. It contains the following sections:

- [Command syntax](#)
- [Command conventions](#)
- [Common parameter values](#)
- [The slot/port \(M4250\) or unit/slot/port \(M4350\) naming convention](#)
- ['no' form of a command](#)
- ['show' commands](#)
- [CLI output filtering](#)
- [Command completion and abbreviation](#)
- [CLI error messages](#)[CLI line-editing conventions](#)
- [Use the CLI help](#)
- [Access the CLI](#)

Command syntax

A command is one or more words that might be followed by one or more parameters. Parameters can be required or optional values.

Some commands, such as **show nsf** and **clear vlan**, do not require parameters. Other commands, such as **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*], require that you supply a value after the command. You must type the parameter values in a specific order, and optional parameters follow required parameters. The following example describes the **route-map** command syntax:

Format	<code>route-map map-tag [permit deny] [sequence-number]</code>

- **route map** is the command name.
- *map-tag* is a parameter (also referred to as an argument) and represents a required value. You must type a value for *map-tag* after typing the **route-map** command name.
- **permit** and **deny** are optional keywords. They are mutually exclusive, so you can type only one. You are not required to enter a value in place of the keyword.
- *sequence-number* is an optional parameter and represents a required value. You must type a value for *sequence-number*.

This command line reference manual lists each command by the command name and provides a brief description of the command. Each command reference also contains the following information:

- Format shows the command keywords and the required and optional parameters.
- Mode identifies the command mode you must be in to access the command.
- Default shows the default value, if any, of a configurable setting on the device.

The **show** commands also contain a description of the information that the command output displays.

Command conventions

The parameters for a command might include mandatory values, optional values, or keyword choices. Parameters are order-dependent. The following table describes the conventions this document uses to distinguish between value types.

Table 1. Parameter Conventions

Symbol	Example	Description
<i>italic font</i>	<i>value</i> or [value]	Indicates a variable value. You must replace the italicized text, which can be placed within curly brackets or square brackets, with an appropriate value, which might be a name or number.
[] square brackets	[keyword]	Indicates an optional parameter.
{ } curly braces	{choice1 choice2}	Indicates that you must select a parameter from the list of choices.
Vertical bars	choice1 choice2	Separates the mutually exclusive choices.
[{ }] Braces within square brackets	[[choice1 choice2]]	Indicates a choice within an optional element. This format is used mainly for complicated commands.

Common parameter values

Parameter values (that is, argument values) might be names (strings) or numbers. To use spaces as part of a name parameter, enclose the name value in double quotes. For example, the expression “System Name with Spaces” forces the system to accept the spaces. Empty strings (“”) are not valid user-defined strings. The following table describes common parameter values and value formatting.

Table 2. Parameter Descriptions

Parameter	Description
ipaddr	This parameter is a valid IPv4 address. You can enter the IP address in the following formats: - a (32 bits) - a.b (8.24 bits) - a.b.c (8.8.16 bits) - a.b.c.d (8.8.8.8) In addition to these formats, the CLI accepts decimal, hexadecimal and octal formats through the following input formats (where <i>n</i> is any valid hexadecimal, octal or decimal number): 0xn (CLI assumes hexadecimal format.) 0n (CLI assumes octal format with leading zeros.) - n (CLI assumes decimal format.)

Table 2. Parameter Descriptions (continued)

Parameter	Description
ipv6-addr	This parameter is a valid IPv6 address. You can enter the IP address in the following formats: - FE80:0000:0000:0000:020F:24FF:FEBF:DBCB - FE80:0:0:0:20F:24FF:FEBF:DBCB - FE80::20F24FF:FEBF:DBCB - FE80:0:0:0:20F:24FF:128:141:49:32 For additional information, refer to RFC 3513.
M4250 series switch: Interface or <i>slot/port</i>	Valid slot and port number separated by a forward slash. The slot is always 0. For example, 0/1 represents port number 1.
M4350 series switch: Interface or <i>unit/slot/port</i>	Valid unit, slot, and port number separated by forward slashes. The unit refers to a stacking configuration. If no stack is configured, the unit is always 0. The slot is always 0. For example, in a switch that does is not a member of a stack, 1/ 0/1 represents port number 1.
Logical Interface	Represents a logical port number. This is applicable in the case of a port-channel (LAG). You can use the logical <i>unit/slot/port</i> to configure the port-channel.
Character strings	Use double quotation marks to identify character strings, for example, "System Name with Spaces". An empty string ("") is not valid.

The slot/port (M4250) or unit/slot/port (M4350) naming convention

An M4250 series switch references physical entities such as ports by using a *slot/port* naming convention.

An M4350 series switch references physical entities such as ports by using a *unit/slot/port* naming convention.

The switch also uses this convention to identify certain logical entities, such as port channel interfaces (link aggregation groups, abbreviated as LAGs).

The port identifies the specific physical port or logical interface.

Table 3. Types of ports

Port Type	Description
M4250 series switch: Physical interfaces	The physical interface number consists of the slot number (which is always 0) followed by a forward slash, and the port number, which is a sequential number starting from 1. Examples: • port 1 is 0/1 • port 2 is 0/2 • port 3 is 0/3 • and so on for other ports
M4350 series switch: Physical interfaces	The physical interface number consists of the switch unit number (from 1 to 8) followed by a forward slash, the slot number (which is always 0) followed by a forward slash, and the port number, which is a sequential number starting from 1. Examples: • Standalone switch: For a switch that is not a member of a stack (that is, a standalone switch), port 1 is 1/0/1, port 2 is 1/0/2, port 3 is 1/0/3, and so on. • Stacked switch: For a switch that is a member of a stack, the port numbering is as follows: - Stack unit 2: port 1 is 2/0/1, port 2 is 2/0/2, port 3 is 2/0/3, and so on - Stack unit 3: port 1 is 3/0/1, port 2 is 3/0/2, port 3 is 3/0/3, and so on - and so on for other stack units, up to stack unit number 8
Logical Interfaces	• Port-channel or Link Aggregation Group (LAG) interfaces are logical interfaces that are used only for bridging functions. • VLAN routing interfaces are used only for routing functions. • Loopback interfaces are logical interfaces that are always up. Note: In the CLI, loopback interfaces do not use the slot/port format (M4250 series switches) or unit/slot/port (M4350 series switches) format. To specify a loopback interface, use the loopback ID.
CPU ports	CPU ports are handled by the driver as one or more physical entities.
Routing VLAN interfaces	This is an interface used for routing functionality: Examples: • VLAN 1 • VLAN 2 • VLAN 3 • and so on

'no' form of a command

The **no** keyword is a specific form of an existing command and does not represent a new or distinct command. Almost every configuration command has a **no** form. In general, use the **no** form to reverse the action of a command or reset a value back to the default. For example, the **no shutdown** configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to reenable a disabled feature or to enable a feature that is disabled by default. Only the configuration commands are available in the **no** form.

'show' commands

All show commands can be issued from any configuration mode (Global Configuration, Interface Configuration, VLAN Configuration, etc.). The show commands provide information about system and feature-specific configuration, status, and statistics.

CLI output filtering

Many CLI show commands include considerable content to display. This can make output confusing and cumbersome to parse through to find the information of desired importance. The CLI Output Filtering feature allows the user, when executing CLI show display commands, to optionally specify arguments to filter the CLI output to display only desired information. The result is to simplify the display and make it easier for the user to find the information the user is interested in.

The main functions of the CLI output filtering feature are:

- **Pagination Control**
 - Supports enabling/disabling paginated output for all **show** CLI commands. When disabled, output is displayed in its entirety. When enabled, output is displayed page-by-page such that content does not scroll off the terminal screen until the user presses a key to continue. --More-- or (q)uit is displayed at the end of each page.
 - When pagination is enabled, press the return key to advance a single line, press q or Q to stop pagination, or press any other key to advance a whole page. These keys are not configurable.

Note: Although some switch **show** commands already support pagination, the implementation is unique per command and not generic to all commands.

- **Output Filtering**
 - "Grep"-like control for modifying the displayed output to only show the user-desired content.
 - Filter displayed output to only include lines containing a specified string match.

- Filter displayed output to exclude lines containing a specified string match.
- Filter displayed output to only include lines including and following a specified string match.
- Filter displayed output to only include a specified section of the content (for example, "interface 0/1") with a configurable end-of-section delimiter.
- String matching should be case insensitive.
- Pagination, when enabled, also applies to filtered output.

The following shows an example of the extensions made to the CLI show commands for the Output Filtering feature.

```
(NETGEAR Switch) #show running-config ?
<cr>                Press enter to execute the command.
|                  Output filter options.
<scriptname>       Script file name for writing active configuration.
all                Show all the running configuration on the switch.
interface          Display the running configuration for specified interface
                  on the switch.
```



```
(NETGEAR Switch) #show running-config | ?
begin              Begin with the line that matches
exclude            Exclude lines that matches
include            Include lines that matches
section            Display portion of lines
```

For new commands for the feature, see [CLI Output Filtering Commands on page 253](#).

Command completion and abbreviation

Command completion finishes spelling the command when you type enough letters of a command to uniquely identify the command keyword. Once you have entered enough letters, press the SPACEBAR or TAB key to complete the word.

Command abbreviation allows you to execute a command when you have entered there are enough letters to uniquely identify the command. You must enter all of the required keywords and parameters before you enter the command.

CLI error messages

If you enter a command and the system is unable to execute it, an error message appears. The following table describes the most common CLI error messages.

Table 4. CLI Error Messages

Message Text	Description
% Invalid input detected at '^' marker.	Indicates that you entered an incorrect or unavailable command. The carat (^) shows where the invalid text is detected. This message also appears if any of the parameters or values are not recognized.
Command not found / Incomplete command. Use ? to list commands.	Indicates that you did not enter the required keywords or values.
Ambiguous command	Indicates that you did not enter enough letters to uniquely identify the command.

CLI line-editing conventions

The following table describes the key combinations you can use to edit commands or increase the speed of command entry. You can access this list from the CLI by entering `help` from the User or Privileged EXEC modes.

Table 5. CLI Editing Conventions

Key Sequence	Description
DEL or Backspace	Delete previous character.
Ctrl-A	Go to beginning of line.
Ctrl-E	Go to end of line.
Ctrl-F	Go forward one character.
Ctrl-B	Go backward one character.
Ctrl-D	Delete current character.
Ctrl-U, X	Delete to beginning of line.
Ctrl-K	Delete to end of line.
Ctrl-W	Delete previous word.
Ctrl-T	Transpose previous character.
Ctrl-P	Go to previous line in history buffer.

Table 5. CLI Editing Conventions (continued)

Key Sequence	Description
Ctrl-R	Rewrites or pastes the line.
Ctrl-N	Go to next line in history buffer.
Ctrl-Y	Prints last deleted character.
Ctrl-Q	Enables serial flow.
Ctrl-S	Disables serial flow.
Ctrl-Z	Return to root command prompt.
Tab, <SPACE>	Command-line completion.
Exit	Go to next lower command prompt.
?	List available commands, keywords, or parameters.

Use the CLI help

Enter a question mark (?) at the command prompt to display the commands available in the current mode.

```
(NETGEAR Switch) >?
```

enable	Enter into user privilege mode.
help	Display help for various special keys.
logout	Exit this session. Any unsaved changes are lost.
password	Change an existing user's password.
ping	Send ICMP echo packets to a specified IP address.
quit	Exit this session. Any unsaved changes are lost.
show	Display Switch Options and Settings.
telnet	Telnet to a remote host.

Enter a question mark (?) after each word you enter to display available command keywords or parameters.

```
(NETGEAR Switch) #network ?
```

ipv6	Configure IPv6 parameters for system network.
javamode	Enable/Disable.
mac-address	Configure MAC Address.
mac-type	Select the locally administered or burnedin MAC address.
mgmt_vlan	Configure the Management VLAN ID of the switch.
parms	Configure Network Parameters of the device.
protocol	Select DHCP, BootP, or None as the network config protocol.

If the help output shows a parameter in angle brackets, you must replace the parameter with a value.

```
(NETGEAR Switch) #network parms ?  
  
<ipaddr>          Enter the IP Address.  
none              Reset IP address and gateway on management interface
```

If there are no additional command keywords or parameters, or if additional parameters are optional, the following message appears in the output:

```
<cr>              Press Enter to execute the command
```

You can also enter a question mark (?) after typing one or more characters of a word to list the available command or parameters that begin with the letters, as shown in the following example:

```
(NETGEAR Switch) #show m?  
  
mac                mac-addr-table          mac-address-table  
mail-server        mbuf                      monitor
```

Access the CLI

You can access the CLI by using a direct console connection or by using a telnet or SSH connection from a remote management host.

For the initial connection, you must use a direct connection to the console port. You cannot access the system remotely until the system has an IP address, subnet mask, and default gateway. You can set the network configuration information manually, or you can configure the system to accept these settings from a BootP or DHCP server on your network. For more information, see [Management Interface Commands on page 63](#).

3

CLI Organization and Command Modes

This chapter describes the CLI organization and command modes. It contains the following sections:

- [CLI command modes](#)
- [How to enter or exit a command mode](#)

CLI command modes

The CLI groups commands into modes according to the command function. Each of the command modes supports specific commands. The commands in one mode are not available until you switch to that particular mode, with the exception of the User EXEC mode commands. You can execute the User EXEC mode commands in the Privileged EXEC mode.

The command prompt changes in each command mode to help you identify the current mode. The following table describes the command modes and the prompts visible in that mode.

Table 6. CLI command modes

Command Mode	Prompt	Mode Description
User EXEC	Switch>	Contains a limited set of commands to view basic system information.
Privileged EXEC	Switch#	Allows you to issue any EXEC command, enter the VLAN mode, or enter the Global Configuration mode.
Global Config	Switch (Config) #	Groups general setup commands and permits you to make modifications to the running configuration.
VLAN Config, also referred to as VLAN Database	Switch (Vlan) #	Groups all the VLAN commands.
Interface Config	M4250 series switch: Switch (Interface <i>slot/port</i>) # M4350 series switch: Switch (Interface <i>unit/slot/port</i>) #	Manages the operation of an interface and provides access to the router interface configuration commands. Use this mode to set up a physical port for a specific logical connection operation.
	Switch (Interface <i>loopback-id</i>) #	
	M4250 series switch: Switch (Interface <i>slot/port -slot/port</i>) # M4350 series switch: Switch (Interface <i>unit/slot/port -unit/slot/port</i>) #	Use this mode to manage the operation of a range of interfaces. For example the prompt may display as follows: M4250 series switch: Switch (Interface 0/1-0/4) # M4350 series switch: Switch (Interface 1/0/1-1/0/4) #
	Switch (Interface lag <i>lag-intf-num</i>) #	Enters LAG Interface configuration mode for the specified LAG.
	Switch (Interface vlan <i>vlan-id</i>) #	Enters VLAN routing interface configuration mode for the specified VLAN ID.

Table 6. CLI command modes (continued)

Command Mode	Prompt	Mode Description
Line Console	Switch (Config-line) #	Contains commands to configure console settings, SSH settings, and outbound Telnet settings, and configure log-in and authentication settings for these types of connections.
Line SSH	Switch (Config-ssh) #	Contains commands to configure SSH login/enable authentication.
Line Telnet	Switch (Config-telnet) #	Contains commands to configure Telnet login/enable authentication.
AAA IAS User Config	Switch (Config-IAS-User) #	Allows password configuration for a user in the IAS database.
Mail Server Config	Switch (Mail-Server) #	Allows configuration of the email server.
Policy Map Config	Switch (Config-policy-map) #	Contains the QoS Policy-Map configuration commands.
Policy Class Config	Switch (Config-policy-classmap) #	Consists of class creation, deletion, and matching commands. The class match commands specify Layer 2, Layer 3, and general match criteria.
Class Map Config	Switch (Config-class-map) #	Contains the QoS class map configuration commands for IPv4.
IPv6 Class-Map Config	Switch (Config-class-map) #	Contains the QoS class map configuration commands for IPv6.
Router OSPF Config	Switch (Config-router) # Note: This mode is supported for an M4350 series switch only.	Contains the OSPF configuration commands.
Router OSPFv3 Config	Switch (Config rtr) # Note: This mode is supported for an M4350 series switch only.	Contains the OSPFv3 configuration commands.
Router RIP Config	Switch (Config-router) #	Contains the RIP configuration commands.
Route Map Config	Switch (Config-route-map) #	Contains the route map configuration commands.
RADIUS Dynamic Authorization Config	Switch (Config-radius-da)	Contains the Radius Dynamic Authorization commands.
MAC Access-list Config	Switch (Config-mac-access-list) #	Lets you create a MAC access list and enter the mode containing MAC access list configuration commands.
IPv4 Access-list Config	Switch (Config-ipv4-acl) #	Lets you create an IPv4 named or extended access list and enter the mode containing IPv4 access list configuration commands.

Table 6. CLI command modes (continued)

Command Mode	Prompt	Mode Description
IPv6 Access-list Config	Switch (Config-ipv6-acl) #	Lets you create an IPv6 named or extended access list and enter the mode containing IPv6 access list configuration commands.
Time-Range Config	Switch (Config-time-range) #	Contains commands to configure time ranges for ACLs.
Management Access-list Config	Switch (Config-macal) #	Lets you create a management access list and enter the mode containing management access list configuration commands.
TACACS Config	Switch (Tacacs) #	Contains commands to configure properties for the TACACS servers.
DHCP Pool Config	Switch (Config-dhcp-pool) #	Contains the DHCP server IP address pool configuration commands.
DHCPv6 Pool Config	Switch (Config-dhcp6s-pool) #	Contains the DHCPv6 server IPv6 address pool configuration commands.
DHCP Class Config	Switch (Config-dhcp-pool) #	Contains the DHCP server IP address class configuration commands.
DHCP Pool Class Config	Switch (Config-dhcp-pool-class) #	Contains the DHCP server IP address pool class configuration commands.
Stack Global Config Mode	Switch (Config-stack) # Note: This mode is supported for an M4350 series switch only.	Allows you to access the Stack Global Config Mode.
ARP Access-List Config Mode	Switch (Config-arp-access-list) #	Contains commands to add ARP ACL rules in an ARP Access List.
VLAN Config	Switch (vlan vlan-id) #	Contains commands to configure private VLAN settings on a VLAN and to configure the RSPAN mode.
ERSPAN Source Session Config	Switch (Config-erspan-src) #	Configure the source interface for ERSPAN and access the ERSPAN Source Session Configuration mode.
ERSPAN Source Session Destination Config	Switch (Config-erspan-src-dst) #	Configure the ERSPAN source and destination IPv4 addresses, session ID, and various characteristics of the packets in the ERSPAN traffic.
ERSPAN Destination Session Config	Switch (Config-erspan-dst) #	Configure the destination interface for ERSPAN and access ERSPAN Destination Session Configuration mode.
ERSPAN Destination Session Source Config	Switch (Config-erspan-dst-src) #	Configure the ERSPAN destination and source IPv4 addresses, session ID, and various characteristics of the packets in the ERSPAN traffic.

Table 6. CLI command modes (continued)

Command Mode	Prompt	Mode Description
Track Config	Switch (Config-track)	Configure settings to track the state of an IP Service Level Agreement (SLA) operation.
IP SLA Config	Switch (Config-ip-sla)	Configure an IP SLA operation.
IP SLA ICMP Echo Config	Switch (Config-ip-sla-echo)	Configure an IP SLA ICMP echo operation.
Captive Portal Config	Switch (Config-CP)	Contains the global captive portal configuration commands.
Captive Portal Instance Config	Switch (Config-CP cp-id)	Contains the captive portal instance configuration commands.
VRRP Config Mode	Switch (Config-if-vrrp) Note: This mode is supported for an M4350 series switch only.	Contains the VRRP or VRRPv3 address family configuration commands.

How to enter or exit a command mode

The following table describes how to enter or exit each mode.

Table 7. CLI mode access and exit

Command Mode	Access Method	Exit or Return to the Previous Mode
User EXEC	This is the first level of access.	To exit, enter logout .
Privileged EXEC	From the User EXEC mode, enter enable .	To exit to the User EXEC mode, enter exit or press Ctrl-Z .
Global Config	From the Privileged EXEC mode, enter configure .	To exit to the Privileged EXEC mode, enter exit , or press Ctrl-Z .
VLAN Config, also referred to as VLAN Database	From the Privileged EXEC mode, enter vlan database .	To exit to the Privileged EXEC mode, enter exit , or press Ctrl-Z .

Table 7. CLI mode access and exit (continued)

Command Mode	Access Method	Exit or Return to the Previous Mode
Interface Config	M4250 series switch: From the Global Config mode, enter: interface <i>slot/port</i> .	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
	M4350 series switch: From the Global Config mode, enter: interface <i>unit/slot/port</i> .	
	M4250 series switch: From the Global Config mode, enter: interface <i>slot/port-slot/port</i> .	
	M4350 series switch: From the Global Config mode, enter: interface <i>unit/slot/port-unit/slot/port</i> .	
	From the Global Config mode, enter: interface <i>loopback-id</i> .	
	From the Global Config mode, enter: interface lag <i>lag-intf-num</i> .	
Line Console	From the Global Config mode, enter: interface <i>loopback-id</i> .	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
	From the Global Config mode, enter: interface lag <i>lag-intf-num</i> .	
	From the Global Config mode, enter: interface <i>loopback-id</i> .	
	From the Global Config mode, enter: interface lag <i>lag-intf-num</i> .	
	From the Global Config mode, enter: interface <i>loopback-id</i> .	
	From the Global Config mode, enter: interface lag <i>lag-intf-num</i> .	
Line SSH	From the Global Config mode, enter line ssh .	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
Line Telnet	From the Global Config mode, enter line telnet .	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
AAA IAS User Config	From the Global Config mode, enter aaa ias-user username <i>name</i> .	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
Mail Server Config	From the Global Config mode, enter mail-server <i>address</i> .	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
Policy-Map Config	From the Global Config mode, enter policy-map <i>policy-name</i> in out .	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
Policy-Class-Map Config	From the Policy Map mode enter class <i>classname</i> .	To exit to the Policy Map Config mode, enter exit . Then, to exit to the Global Config mode, enter exit again. To return to the Privileged EXEC mode, enter Ctrl-Z .

Table 7. CLI mode access and exit (continued)

Command Mode	Access Method	Exit or Return to the Previous Mode
Class-Map Config	From the Global Config mode, enter class-map , and specify the optional keyword ipv4 to specify the Layer 3 protocol for this class. See class-map on page 1287 for more information.	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
IPv6-Class-Map Config	From the Global Config mode, enter class-map and specify the optional keyword ipv6 to specify the Layer 3 protocol for this class. See class-map on page 1287 for more information.	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
Router OSPF Config	From the Global Config mode, enter router ospf . Note: This mode is supported for an M4350 series switch only.	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
Router OSPFv3 Config	From the Global Config mode, enter ipv6 router ospf . Note: This mode is supported for an M4350 series switch only.	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
Router RIP Config	From the Global Config mode, enter router rip .	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
Route Map Config	From the Global Config mode, enter route-map <i>map-tag</i> .	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
RADIUS Dynamic Authorization Config	From the Global Config mode, enter aaa server radius dynamic-author .	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
MAC Access-list Config	From the Global Config mode, enter mac access-list extended <i>name</i> .	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
IPv4 Access-list Config	From the Global Config mode, enter ip access-list <i>name</i> .	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
Time-Range Config	From the Global Config mode, enter time-range <i>name</i> .	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
IPv6 Access-list Config	From the Global Config mode, enter ipv6 access-list <i>name</i> .	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
Management Access-list Config	From the Global Config mode, enter management access-list <i>list-name</i> .	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .

Table 7. CLI mode access and exit (continued)

Command Mode	Access Method	Exit or Return to the Previous Mode
TACACS Config	From the Global Config mode, enter tacacs-server host <i>ip-addr</i> , where <i>ip-addr</i> is the IP address of the TACACS server on your network.	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
DHCP Pool Config	From the Global Config mode, enter ip dhcp pool <i>pool-name</i> .	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
DHCPv6 Pool Config	From the Global Config mode, enter ipv6 dhcp pool <i>pool-name</i> .	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
DHCP Class Config	From the Global Config mode, enter ip dhcp class <i>class-name</i> .	To exit to the Global Config mode, enter exit . To return to the Privileged EXEC mode, enter Ctrl-Z .
DHCP Pool Class Config	From the DHCP Pool Config mode, enter class <i>name</i>	To exit to the DHCP Pool Config mode, enter exit . Then, to exit to the Global Config mode, enter exit again. To return to the Privileged EXEC mode, enter Ctrl-Z .
Stack Global Config Mode	From the Global Config mode, enter the stack command. Note: This mode is supported for an M4350 series switch only.	To exit to the Global Config mode, enter the exit command. To return to the Privileged EXEC mode, enter Ctrl-Z .
ARP Access-List Config Mode	From the Global Config mode, enter arp access-list .	To exit to the Global Config mode, enter the exit command. To return to the Privileged EXEC mode, enter Ctrl-Z .
VLAN Config	From the Global Config mode, enter vlan <i>vlan-id</i> .	To exit to the Global Config mode, enter the exit command. To return to the Privileged EXEC mode, enter Ctrl-Z .
ERSPAN Source Session Config	From the Global Config mode, enter monitor session <i>session-id</i> type erspan-source .	To exit to the Global Config mode, enter the exit command. To return to the Privileged EXEC mode, enter Ctrl-Z .
ERSPAN Source Session Destination Config	From the ERSPAN Source Session Configuration Mode, enter destination .	To exit to the ERSPAN Source Session Destination Config mode, enter exit . Then, to exit to the Global Config mode, enter exit again. To return to the Privileged EXEC mode, enter Ctrl-Z .
ERSPAN Destination Session Config	From the Global Config mode, enter monitor session <i>session-id</i> type erspan-destination .	To exit to the Global Config mode, enter the exit command. To return to the Privileged EXEC mode, enter Ctrl-Z .
ERSPAN Destination Session Source Config	From the ERSPAN Destination Session Configuration Mode, enter source .	To exit to the ERSPAN Destination Session Source Config mode, enter exit . Then, to exit to the Global Config mode, enter exit again. To return to the Privileged EXEC mode, enter Ctrl-Z .

Table 7. CLI mode access and exit (continued)

Command Mode	Access Method	Exit or Return to the Previous Mode
Track Config	From the Global Config mode, enter track <i>object-number</i> ip sla <i>operation-number</i> .	To exit to the Global Config mode, enter the exit command. To return to the Privileged EXEC mode, enter Ctrl-Z .
IP SLA Config	From the Global Config mode, enter ip sla <i>operation-number</i> .	To exit to the Global Config mode, enter the exit command. To return to the Privileged EXEC mode, enter Ctrl-Z .
IP SLA ICMP Echo Config	From IP SLA Config mode, enter icmp-echo <i>destination-ip-address</i> .	To exit to the IP SLA ICMP Echo Config mode, enter exit . Then, to exit to the Global Config mode, enter exit again. To return to the Privileged EXEC mode, enter Ctrl-Z .
Captive Portal Config	From Global Config mode, enter captive-portal .	To exit to the Global Config mode, enter the exit command. To return to the Privileged EXEC mode, enter Ctrl-Z .
Captive Portal Instance Config	From the Captive Portal Config mode, enter configuration <i>cp-id</i> .	To exit to the Captive Portal Instance Config mode, enter exit . Then, to exit to the Global Config mode, enter exit again. To return to the Privileged EXEC mode, enter Ctrl-Z .
VRRP Config Mode	From the Interface Config mode, enter vrrp <i>group-id</i> address-family { ipv4 ipv6 }. Note: This mode is supported for an M4350 series switch only.	To exit to the Interface Config mode, enter exit . Then, to exit to the Global Config mode, enter exit again. To return to the Privileged EXEC mode, enter Ctrl-Z .

4

Stacking Commands

This chapter describes the stacking commands.

Note: Stacking commands are supported on the M4350 series switches only. The M4250 series switches do not support stacking.

This chapter contains the following sections:

- [Dedicated Port Stacking Commands](#)
- [Stack Port Commands](#)
- [Stack Firmware Synchronization and Copy Commands](#)
- [Nonstop Forwarding Commands for Stack Configuration](#)

The commands in this chapter are in two functional groups:

- **Show commands.** Display switch settings, statistics, and other information.
- **Configuration commands.** Configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.

Note: The primary management unit is the switch that controls the stack.

Dedicated Port Stacking Commands

This section describes the commands you use to configure dedicated port stacking.

stack

M4350

Use this command to set the mode to Stack Global Config.

Default	None
Format	stack
Mode	Global Config

member (Stack Global Config)

M4350

Use this command to add a switch to a stack. The *unit* is the switch identifier of the switch to be added to the stack. The *switchindex* is the index into the database of the supported switch types, indicating the type of the switch being preconfigured. The *switchindex* is a 32-bit integer. You issue this command on the primary management unit.

Default	None
Format	member <i>unit</i> <i>switchindex</i>
Mode	Stack Global Config

Note: You can obtain the switch index by issuing the **show supported switchtype** command in User EXEC mode.

no member

Use this command to remove a switch from a stack. The *unit* is the switch identifier of the switch to be removed from the stack. You issue this command on the primary management unit.

Format	no member <i>unit</i>
Mode	Stack Global Config

switch priority

M4350

Use this command to configure the ability of a switch to become the primary management unit. The *unit* is the switch identifier. The *value* is the preference parameter that lets you specify the priority of one backup switch over another. The range for priority is 1 to 15. The switch with the highest priority value becomes the primary management unit if the active primary management unit fails. The switch priority defaults to the hardware management preference value 1. Switches without the hardware capability to become the primary management unit are not eligible for management.

Default	Enabled
Format	<code>switch unit priority value</code>
Mode	Global Config

switch renumber

M4350

Use this command to change the switch identifier for a switch in the stack. The *oldunit* is the current switch identifier on the switch whose identifier is to be changed. The *newunit* is the updated value of the switch identifier. When you issue the command, the switch is configured with the configuration information for the new switch, if any. The old switch configuration information is retained, however the old switch becomes operationally unplugged. You issue this command on the primary management unit.

Note: If the management unit is renumbered, the running configuration is no longer applied (that is, the stack functions as if the running configuration is cleared).

Default	None
Format	<code>switch oldunit renumber newunit</code>
Mode	Global Config

movemanagement (Stack Global Config)

M4350

Use this command to move the primary management switch functionality from one switch to another. The *fromunit* is the switch identifier on the current primary management unit. The *tounit* is the switch identifier on the new primary management unit. When you issue the command, 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, you must perform all stack management capability on the new primary

management unit. To preserve the current configuration across a stack move, issue the **copy system:running-config nvram:startup-config** command in Privileged EXEC mode before performing the stack move. A stack move causes all routes and layer 2 addresses to be lost. You issue this command on the primary management unit. The system prompts you to confirm the management move.

Note: The **movemanagement** command does not perform nonstop forwarding (NSF). To move the management unit to the backup unit, issue the **initiate failover** command instead. For more information, see [initiate failover \(for stack configuration\) on page 55](#).

Default	None
Format	<code>movemanagement fromunit tounit</code>
Mode	Stack Global Config

standby

M4350

Use this command to configure a unit as a standby management unit (STBY). The *unit number* is the unit number that must become the standby management unit. The *unit number* must be a valid unit number.

Default	None
Format	<code>standby unit number</code>
Mode	Stack Global Config

Note: The standby management unit cannot be the current management unit. The standby unit must be a management-capable unit.

no standby

Use this command to let the switch run the auto standby management unit.

Format	<code>no standby</code>
Mode	Stack Global Config

slot (for stack configuration)

M4250 (supported for a non-stack configuration)

M4350

Use this command to configure a slot in the system. The *unit/slot/port* identifies the slot. The *cardindex* is the index into the database of the supported card types, indicating the type of the card that is being preconfigured in the specified slot. The *cardindex* is a 32-bit integer. If a card is present in the slot that is unconfigured, the configured information is deleted and the slot is reconfigured with default information for the card.

Default	None
Format	<i>slot unit/slot/port cardindex</i>
Mode	Global Config

Note: You can obtain the card index by issuing the **show supported cardtype** command in User EXEC mode.

no slot

Use this command to remove configured information from an existing slot in the system.

Format	<i>no slot unit/slot/port cardindex</i>
Mode	Global Config

Note: You can obtain the card index by issuing the **show supported cardtype** command in User EXEC mode.

set slot disable (for stack configuration)

M4250 (supported for a non-stack configuration)

M4350

Use this command to configure the administrative mode for a specified slot or for all slots. If you specify **a11**, the command is applied to all slots, otherwise the command is applied to the slot that is identified by *unit/slot/port*.

If a card or other module is present in the slot, the administrative mode is applied to the contents of the slot. If the slot is empty, the administrative mode is applied to any module that

is inserted into the slot. If a card is disabled, all the ports on the device are operationally disabled and shown as “unplugged” on management screens.

Default	None
Format	<code>set slot disable [unit/slot/port all]</code>
Mode	Global Config

no set slot disable

Use this command to remove the administrative mode for a specified slot or for all slots. If you specify **a11**, the command removes the administrative mode from all slots, otherwise the command removes the administrative mode from the slot that is identified by *unit/slot/port*.

If a card or other module is present in the slot, the administrative mode removes the configuration from the contents of the slot. If the slot is empty, the administrative mode removes the configuration from any module inserted into the slot. If a card is disabled, all the ports on the device are operationally disabled and shown as “unplugged” on management screens.

Format	<code>no set slot disable [unit/slot/port all]</code>
Mode	Global Config

set slot power (for stack configuration)

M4250 (supported for a non-stack configuration)

M4350

Use this command to configure the power mode for a specified slot or for all slots and allows power to be supplied to the cards that are located in the slots. If you specify **a11**, the command is applied to all slots, otherwise the command is applied to the slot that is identified by *unit/slot/port*.

Use this command when you install or remove cards. If a card or other module is present in the slot, the power mode is applied to the contents of the slot. If the slot is empty, the power mode is applied to any card inserted into the slot.

Default	None
Format	<code>set slot power [unit/slot/port all]</code>
Mode	Global Config

no set slot power

Use this command to remove the power mode for a specified slot or for all slots and prohibits power from being supplied to the cards that are located in the slots. If you specify **a11**, the

command prohibits power to all slots, otherwise the command prohibits power to the slot that is identified by *unit/slot/port*.

Use this command when you install or remove cards. If a card or other module is present in the slot, power is prohibited to the contents of the slot. If the slot is empty, power is prohibited to any card inserted into the slot.

Format	<code>no set slot power [unit/slot/port all]</code>
Mode	Global Config

trunk-hashmode

M4350

This command configures load-balancing mode on all trunks across the switches in a stacking topology. The *id* argument specifies the type of load-balancing (hashing mode).

Default	3
Format	<code>trunk-hashmode id</code>
Mode	Stack Global Config

Parameter	Definition
1	Source MAC, VLAN, EtherType, and incoming port associated with the packet.
2	Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
3	Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
4	Source IP and Source TCP/UDP fields of the packet.
5	Destination IP and Destination TCP/UDP Port fields of the packet.
6	Source/Destination IP and source/destination TCP/UDP Port fields of the packet.
7	Enhanced hashing mode.

no trunk-hashmode

This command disables load-balancing mode on all trunks across the switches in a stacking topology

Format	<code>no trunk-hashmode</code>
Mode	Stack Global Config

reload (for stack configuration)

M4250 (supported for a non-stack configuration)

M4350

Use this command to reset the entire stack or the identified unit. The *unit* is the switch identifier. The system prompts you to confirm that you want to reset the switch.

Default	None
Format	reload [<i>unit</i>]
Mode	User EXEC

stack-status sample-mode

M4350

Use this command to configure the global status management mode and, as an option, the sample size. The mode and sample size parameters are applied globally to all units in the stack. The default sampling mode of the operation is cumulative, which tacks the sum of the received time stamp offsets cumulatively. You can also select the history sampling mode, which tracks the history of the received timestamps.

The sample size indicates the maximum number of samples that must be kept. The range for the *number* value for **max-samples** is from 100 to 500.

Note: The **stack-status sample-mode** command is implemented as part of a serviceability functionality and therefore not expected to be persistent across reloads. The configuration is not visible in the running configuration under any circumstances. When you issue the command, the configuration is applied to all the members that are part of the stack. After you issue the command, the configuration is not applied to new members that you add to the stack.

Default	The default for sampling mode is cumulative. The default for max-samples is 300.
Format	stack-status sample-mode {cumulative history} [max-samples <i>number</i>]
Mode	Stack Global Config

The following command sets the sampling mode to cumulative:

```
(NETGEAR Switch) #configure
(NETGEAR Switch) (Config)#stack
(NETGEAR Switch) (Config-stack)# stack-status sample-mode cumulative
```

Command example:

The following command sets the sampling mode to history and the sample size to the default.

```
(NETGEAR Switch) #configure
(NETGEAR Switch) (Config)#stack
(NETGEAR Switch) (Config-stack)#stack-status sample-mode history
```

Command example:

The following command sets the sampling mode to history and sample size to 100.

```
(NETGEAR Switch) #configure
(NETGEAR Switch) (Config)#stack
(NETGEAR Switch) (Config-stack)#stack-status sample-mode history max-samples 100
```

show slot

M4250 (supported for a non-stack configuration)

M4350

Use this command to display information about all the slots in the system or about a specific slot.

Format	show slot [<i>unit/slot/port</i>]
Mode	User EXEC Privileged EXEC
Term	Definition
Slot	The slot identifier in the unit/slot/port format.
Status	The slot status, which can be Empty, Full, or Error.
Admin State	The slot administrative mode (Enabled or Disabled).
Power State	The slot power mode (Enabled or Disabled).
Configured Card Model ID	The preconfigured card type.
Inserted Card Model ID	The actually installed card type.
Seral Number	Serial number of the card, if present.
Pluggable	Indicates if the card is pluggable.
Power Down	Indicates if the slot can be powered down.

Command example:

This example shows the output of the **show slot** command:

```
(NETGEAR Switch)>show slot
```

Slot	Status	Admin State	Power State	Configured Card Model ID	Inserted Card Model ID	Pluggable	Power Down
1/0	Full	Enable	Enable	M4350-16V4C	M4350-16V4C	No	No

For a switch with multiple slots, you can change the configuration for a slot from a set type of port card to a dynamic port card by entering the **no slot *unit/slot/port*** command. For example, to remove the configuration of slot 2 so that the slot can enter any of the supported port cards dynamically, enter the **no slot 1/2** command.

Note: The output of the **show slot** command shows only the port cards in the slots that are populated or are configured for a particular type of port card.

If you supply a value for *unit/slot/port*, the following additional information displays:

Term	Definition
Inserted Card Model Identifier	The model identifier of the card inserted in the slot. The model identifier is a 32-character field used to identify a card. This field is displayed only if the slot is populated.
Inserted Card Description	The card description. This field is displayed only if the slot is populated.
Configured Card Description	The card description of the card preconfigured in the slot.

show stack-hashmode

M4350

Use this command to display the dynamically-formed trunks in a stacking system and configured load-balancing mode for each of these trunks.

Format	show stack-hashmode
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch)show stack-hashmode
```

Unit	Trunk ID	Member Ports	Configured Hash Mode	Oper Hash Mode
---	-----	-----	-----	-----
1	128	1/0/27, 1/0/28	2 (Dst MAC Address)	2 (Dst MAC Address)
2	128	2/0/27, 2/0/28	1 (Src MAC Address)	1 (Src MAC Address)
2	129	2/0/25, 2/0/26	2 (Dst MAC Address)	2 (Dst MAC Address)

show stack-status**M4350**

Use this command to display the stack unit's received heartbeat message timings and the dropped or lost statistics for the specified unit.

Use the following optional keywords to specify the command output:

- *number*. The output displays for a specific unit in the stack. The value for *number* can be from 1 to 8.
- **all**. The output displays for all units in the stack.

Use the optional keyword **clear** to remove the statistics of the stack heartbeat message.

```
Format      show stack stack-status [number | all] [clear]
```

```
Mode        Privileged EXEC
```

Term	Definition
Current	The time at which the heartbeat message was received.
Average	The average time of the heartbeat messages that were received.
Min	The minimum time of the heartbeat messages that were received.
Max	The maximum time of the heartbeat messages that were received.
Dropped	The number of heartbeat messages that were dropped or lost.

Command example:

This example dumps the stack unit heartbeat status information of the specified unit:

```
(NETGEAR Switch) #show stack-status
Stack Unit 1 Status
Sampling Mode: Cumulative Summing
-----
Unit Current Average Min Max Dropped
-----
```

show supported cardtype (for stack configuration)

M4250 (supported for a non-stack configuration)

M4350

Use this command to display information about all card types or specific card types that are supported in the switch.

Format	show supported cardtype [<i>cardindex</i>]

Mode	User EXEC

If you do not supply a value for *cardindex*, the following output displays:

Term	Definition
Card Index (CID)	The index in the database for the supported card types. This index is used when you preconfigure a slot.
Card Model Identifier	The model identifier for the supported card type.

If you supply a value for *cardindex*, the following output displays:

Term	Definition
Card Type	The 32-bit numeric card type for the supported card.
Model Identifier	The model identifier for the supported card type.
Card Description	The description for the supported card type.

show switch

M4350

Use this command to display information about all units in the stack or about a single unit if you specify the unit value. For units that lack a matching stack template ID and can therefore not join the stack, the switch status is shown as “STM Mismatch.”

Format	show switch [<i>unit</i>]

Mode	Privileged EXEC

Term	Definition
Switch	The unit identifier assigned to the switch.

If you do not specify a value for *unit*, the following information displays:

Term	Definition
Management Status	Indicates whether the switch is the primary management unit, a stack member, or the status is unassigned.
Preconfigured Model Identifier	The model identifier of a preconfigured switch ready to join the stack. The model identifier is a 32-character field that is assigned by the device manufacturer to identify the device.
Plugged-In Model Identifier	The model identifier of the switch in the stack. The model identifier is a 32-character field that is assigned by the device manufacturer to identify the device.
Switch Status	The switch status. Possible values for this state are: OK, Unsupported, Code Mismatch, Config Mismatch, or Not Present. A mismatch indicates that a stack unit is running a different firmware version, Switch Database Management (SDM) template, or configuration than the management unit. The SDM Mismatch status indicates that the unit joined the stack, but is running a different SDM template than the management unit. This status is temporary; the stack unit automatically reloads using the template that is running on the stack manager. If a Stacking Firmware Synchronization operation is in progress, the status is shown as Updating Code.
Code Version	The detected version of code on the switch.

Command example:

```
(NETGEAR Switch) #show switch
      Management Standby   Preconfig   Plugged-in   Switch   Code
SW  Switch   Status   Model ID   Model ID   Status   Version
---  ---
1   Stack Mbr           Platform v1   Platform v1   STM Mismatch  10.17.15.8
2   Mgmt Sw             Platform v2   Platform v2   OK           10.17.15.8
```

If you specify a value for *unit*, the following information displays:

Term	Definition
Management Status	Indicates whether the switch is the primary management unit, a stack member, or the status is unassigned.
Hardware Management Preference	The hardware management preference of the switch. The hardware management preference can be disabled or unassigned.
Admin Management Preference	The administrative management preference value assigned to the switch. This preference value indicates how likely the switch is selected as the primary management unit.
Switch Type	The 32-bit numeric switch type.
Model Identifier	The model identifier for this switch. The model identifier is a 32-character field that is assigned by the device manufacturer to identify the device.

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Switch Status	The switch status. Possible values are OK, Unsupported, Code Mismatch, Config Mismatch, or Not Present.
Switch Description	The switch description.
Expected Code Version	The expected firmware version.
Detected Code Version	The version of firmware that is running on this switch. If the switch is not present and the data is from the preconfiguration, the firmware version is None.
Detected Code in Flash	The version of the firmware that is currently stored in flash memory on the switch. The firmware executes after the switch is reset. If the switch is not present and the data is from the preconfiguration, the firmware version is None.
SFS Last Attempt Status	The stack firmware synchronization status in the last attempt for the specified unit.
Stack Template ID	The ID of the stack template. For example: 3.
Stack Template Description	The stack template description. For example: v1 and v2 Mix.
Up Time	The system up time.

Command example:

```
(Netgear Switch) #show switch 1

Switch..... 1
Management Status..... Management Switch
Hardware Management Preference.... Unassigned
Admin Management Preference..... Unassigned
Switch Type..... 0xd6064004
Preconfigured Model Identifier.... M4350-16V4C
Plugged-in Model Identifier..... M4350-16V4C
Switch Status..... OK
Switch Description..... M4350-16V4C
Detected Code in Flash..... 14.0.0.2
CPLD version..... 0x1
SFS Last Attempt Status..... None
Serial Number..... 4G115B1234567
Up Time..... 2 days 3 hrs 24 mins 33 secs
```

show supported switchtype (for stack configuration)

M4250 (supported for a non-stack configuration)

M4350

Use this command to display information about all supported switch types or about a specific switch type.

Format	show supported switchtype [<i>switchindex</i>]
Modes	User EXEC Privileged EXEC

If you do not supply a value for *switchindex*, the following output displays:

Term	Definition
Switch Index (SID)	The index in the database of supported switch types. This index is used when you preconfigure a member to be added to the stack.
Model Identifier	The model identifier for the supported switch type.
Management Preference	The management preference value of the switch type.
Code Version	The firmware load target identifier of the switch type.

If you supply a value for *switchindex*, the following output displays:

Term	Definition
Switch Type	The 32-bit numeric switch type for the supported switch.
Model Identifier	The model identifier for the supported switch type.
Switch Description	The description for the supported switch type.

Stack Port Commands

This section describes the commands you use to view and configure stack port information.

stack-port

M4350

Use this command to set stacking for a specified port to either **stack** or **ethernet** mode.

Default	stack
Format	stack-port <i>unit/slot/port</i> {ethernet stack}
Mode	Stack Global Config

show stack-port

Use this command to display summary stack-port information for all interfaces.

Format	show stack-port
Mode	Privileged EXEC

For each interface:

Term	Definition
Unit	The unit number.
Interface	The slot and port numbers.
Configured Stack Mode	Stack or Ethernet.
Running Stack Mode	Stack or Ethernet.
Link Status	The status of the link.
Link Speed	The speed (in Gbps) of the stack port link.

show stack-port counters

M4350

Use this command to display summary data counter information for all interfaces.

Use the following optional keywords to specify the command output:

- *number*. The output displays for a specific unit in the stack. The value for *number* can be from 1 to 8.
- **all**. The output displays for all units in the stack.

Format `show stack-port counters [number | all]`

Mode Privileged EXEC

Term	Definition
Unit	The unit number.
Interface	The slot and port numbers.
Tx Data Rate	The trashing data rate in megabits per second on the stacking port.
Tx Error Rate	The platform-specific number of transmit errors per second.
Tx Total Error	The platform-specific number of total transmit errors since power-up.
Rx Data Rate	The received data rate in megabits per second on the stacking port.
Rx Error Rate	The platform-specific number of received errors per second.
Rx Total Errors	The platform-specific number of total received errors since power-up.
Link Flaps	The number of up and down events for the link since the system bootup.

This example shows the stack ports and associated statistics of unit 2.

(NETGEAR Switch) `#show stack-port counters 2`

Unit	Interface	-----TX-----			-----RX-----			Link Flaps
		Data Rate (Mb/s)	Error Rate (Errors/s)	Total Errors	Data Rate (Mb/s)	Error Rate (Errors/s)	Total Errors	
2	0/53	0	0	0	0	0	0	0
2	0/54	0	0	0	0	0	0	0
2	0/55	0	0	0	0	0	0	0
2	0/56	0	0	0	0	0	0	0

show stack-port diag

M4350

Note: This command is intended only for field application engineers (FAEs) and developers.

Use this command to display front panel stacking diagnostics for each port. An FAE can advise on the necessity to run this command and capture this information. In verbose mode,

the statistics and counters for RPC, transport, CPU, and transport RX/TX modules are displayed.

Use the following optional keywords to specify the command output:

- *number*. The output displays for a specific unit in the stack. The value for *number* can be from 1 to 8.
- **a11**. The output displays for all units in the stack.

Format	show stack-port diag [<i>number</i> all] [verbose]
Mode	Privileged EXEC
Term	Definition
Unit	The unit number.
Interface	The slot and port numbers.
Diagnostic Entry1	80 character string used for diagnostics.
Diagnostic Entry2	80 character string used for diagnostics.
Diagnostic Entry3	80 character string used for diagnostics.
TBYT	Transmitted bytes.
TPKT	Transmitted packets.
TFCS	Transmitted FCS error frame counter.
TERR	Transmitted error (set by system) counter
RBYT	Received bytes.
RPKT	Received packets.
RFCS	Received FCS error frame counter.
RFRG	Received fragment counter.
RJBR	Received jabber frame counter.
RUND	Received undersized frame counter.
ROVR	Received oversized frame counter.
RUNT	Received RUNT frame counter.

Command example:

This example displays the stack ports and associated statistics of specified unit or all units.

```
(NETGEAR Switch) #show stack-port diag 1

1 - 0/53:
RBYT:27ed9a7b RPKT:bca1b TBYT:28a0739e TPKT:c93ee
RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0
```

```
TFCS:0 TERR:0
```

```
1 - 0/54:
```

```
RBYT:8072ed RPKT:19a66 TBYT:aecfb80 TPKT:66e4d
```

```
RFCS:6e RFRG:4414 RJBR:0 RUND:c19 RUNT:af029b1
```

```
TFCS:0 TERR:0
```

```
1 - 0/55:
```

```
RBYT:0 RPKT:0 TBYT:ae8 TPKT:23
```

```
RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0
```

```
TFCS:0 TERR:0
```

```
1 - 0/56:
```

```
RBYT:0 RPKT:0 TBYT:ae8 TPKT:23
```

```
RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0
```

```
TFCS:0 TERR:0
```

Command example:

This example displays a dump of the RPC, Transport (ATP, Next Hop, and RLink), and CPU Transport Rx/Tx module statistics for Unit 2.

```
(NETGEAR Switch) #show stack-port diag 2 verbose
-----
HPC RPC statistics/counters from unit..2
-----
Registered Functions..... 58
Client Requests..... 0
Server Requests..... 0
Server Duplicate Requests..... 0
Server Replies..... 0
Client Remote Tx..... 0
Client Remote Retransmit Count..... 0
Tx without Errors..... 0
Tx with Errors..... 0
Rx Timeouts..... 0
Rx Early Exits..... 0
Rx Out of Sync..... 0
No Buffer..... 0
Collect Sem Wait Count..... 0
Collect Sem Dispatch Count..... 0

-----
RPC statistics/counters from unit..2
-----
Client RPC Requests Count..... 3
Client RPC Reply Count..... 0
```

Fully Managed Switches M4250 and M4350 Series

```
Client RPC Fail to xmit Count..... 0
Client RPC Response Timedout Count..... 3
Client RPC Missing Requests..... 0
Client RPC Detach/Remove Count..... 0
Client RPC Current Sequence Number..... 3
Server RPC Request Count..... 0
Server RPC Reply Count..... 0
Server RPC Processed Transactions..... 0
Server RPC Received Wrong Version Req..... 0
Server RPC No Handlers..... 0
Server RPC Retry Transmit Count..... 0
Server RPC Repetitive Tx Errors..... 0

-----
ATP statistics/counters from unit..2
-----
Transmit Pending Count..... 2
Current number of TX waits..... 2
Rx transactions created..... 145
Rx transactions freed..... 145
Rx transactions freed(raw)..... 0
Tx transactions created..... 290
BET Rx Dropped Pkts Count..... 0
ATP Rx Dropped Pkts Count..... 0
Failed to Add Key Pkt Count..... 0
Source Lookup Failure Count..... 0
Old Rx transactions Pkts drop Count..... 0
Nr of CPUs found in ATP communication..... 2

-----
CPU Transport statistics/counters from unit..2
-----
State Initialization..... Done
Rx Setup..... Done
Tx Setup..... Done
Tx CoS[0] Reserve..... 100
Tx CoS[1] Reserve..... 100
Tx CoS[2] Reserve..... 100
Tx CoS[3] Reserve..... 100
Tx CoS[4] Reserve..... 60
Tx CoS[5] Reserve..... 40
Tx CoS[6] Reserve..... 20
Tx CoS[7] Reserve..... 0
Tx Pkt Pool Size..... 200
Tx Available Pkt Pool Size..... 198
Tx failed/error Count..... 0
Rx Pkt Pool Size..... 8
```

```
-----
Next Hop statistics/counters from unit..2
-----
```

```
State Initialization..... Done
Component Setup..... Done
Thread Priority..... 100
Rx Priority..... 105
Local CPU Key..... 00:24:81:d0:0f:c7
MTU Size..... 2048
Vlan Id..... 4094
CoS Id..... 7
Internal Priority for pkt transmission..... 7
Rx Pkt Queue Size..... 256
Tx Pkt Queue Size..... 64
Rx Pkt Dropped Count..... 0
Tx Failed Pkt Count..... 0
```

```
-----
RLink statistics/counters from unit..2
-----
```

```
State Initialization..... Done
L2 Notify In Pkts..... 0
L2 Notify In Pkts discarded..... 0
L2 Notify Out Pkts ..... 0
L2 Notify Out Pkts discarded..... 0
Linkscan In Pkts..... 0
Linkscan In Pkts discarded..... 0
Linkscan Out Pkts ..... 0
Linkscan Out Pkts discarded..... 0
Auth/Unauth In Callbacks..... 0
Auth/Unauth In Callbacks discarded..... 0
Auth/Unauth Out Callbacks..... 0
Auth/Unauth Out Callbacks discarded..... 0
RX Tunnelling In Pkts..... 0
RX Tunnelling In Pkts discarded..... 0
RX Tunnelling Out Pkts..... 0
RX Tunnelling Out Pkts discarded..... 0
OAM Events In..... 0
OAM Events In discarded..... 0
OAM Events Out..... 0
OAM Events Out discarded..... 0
BFD Events In..... 0
BFD Events In discarded..... 0
BFD Events Out..... 0
BFD Events Out discarded..... 0
```

```

Fabric Events In..... 0
Fabric Events In discarded..... 0
Fabric Events Out..... 0
Fabric Events Out discarded..... 0
Scan Add Requests In..... 0
Scan Del Requests In..... 0
Scan Notify(Run Handlers) Out..... 0
Scan Notify(Traverse Processing)..... 0

```

show stack-port stack-path

M4350

Use this command to display the route that a packet takes to reach its destination. This command lets you display the stack path to see if an error or packets loss occurs.

Use the following optional keywords to specify the command output:

- *source-unit*. The output displays for a specific source unit in the stack. The value for *source-unit* can be from 1 to 8.
- **a11**. The output displays for all units in the stack.
- *destination-unit*. The output displays for a specific source unit in the stack. The value for *destination-unit* can be from 1 to 8.

Format	show stack-port stack-path [<i>source-unit</i> all] [<i>destination-unit</i>]
Mode	Privileged EXEC

Stack Firmware Synchronization and Copy Commands

Stack firmware synchronization (SFS) provides an automatic mechanism to synchronize the firmware on all stack members whose firmware version differs from the version running on the stack manager. This operation can result in either an upgrade or downgrade of firmware on the mismatched stack member. However, this operation does not attempt to synchronize the stack to the latest firmware in the stack.

boot auto-copy-sw (for stack firmware synchronization)

M4350

Use this command to enable stack firmware synchronization.

Default	Disabled
Format	<code>boot auto-copy-sw</code>
Mode	Privileged EXEC

no boot auto-copy-sw

Use this command to disable stack firmware synchronization.

Format	<code>no boot auto-copy-sw</code>
Mode	Privileged EXEC

boot auto-copy-sw trap (for stack firmware synchronization)

M4350

Use this command to send SNMP traps related to stack firmware synchronization.

Default	Enabled
Format	<code>boot auto-copy-sw trap</code>
Mode	Privileged EXEC

no boot auto-copy-sw trap

Use this command to disable sending SNMP traps related to stack firmware synchronization.

Format	<code>no boot auto-copy-sw trap</code>
Mode	Privileged EXEC

boot auto-copy-sw allow-downgrade (for stack firmware synchronization)

M4350

Use this command to enable downgrading of the firmware version on the stack member if the firmware version on the manager is older than the firmware version on the member.

Default	Enabled
Format	<code>boot auto-copy-sw allow-downgrade</code>
Mode	Privileged EXEC

no boot auto-copy-sw allow-downgrade

Use this command to prevent downgrading of the firmware version on the stack member if the firmware version on the manager is older than the firmware version on the member.

Format	no boot auto-copy-sw allow-downgrade

Mode	Privileged EXEC

copy unit

M4350

Use this command to copy a source image (1 or 2) to a destination image (1 or 2) on a specific stack member or on all stack members.

Format	copy image {1 2} unit {all unit-number} image {1 2}

Mode	Privileged EXEC

copy nvram:core-dum unit

M4350

Use this command to export a core dump file from a source on a local file system to a specific stack member. Specifying the source is optional.

Format	copy nvram:core-dump unit <i>number filename</i> [source { <i>ip-address</i> <i>unit/slot/port</i> loopback <i>number</i> serviceport vlan <i>vlan-id</i> }]

Mode	Privileged EXEC

copy nvram:cpu-pkt-capture.pcap unit

M4350

Use this command to copy a CPU packets capture file from a source on a local file system to a specific stack member. Specifying the source is optional.

Format	copy nvram:cpu-pkt-capture.pcap unit <i>number filename</i> [source { <i>ip-address</i> <i>unit/slot/port</i> loopback <i>number</i> serviceport vlan <i>vlan-id</i> }]

Mode	Privileged EXEC

copy nvram:tech-support unit

M4350

Use this command to copy a tech support file from a source on a local file system to a specific stack member. Specifying the source is optional.

Format	<code>copy nvram:tech-support unit <i>number filename</i> [source {<i>ip-address</i> <i>unit/slot/port</i> <i>loopback number</i> <i>serviceport</i> <i>vlan vlan-id</i>}]</code>
Mode	Privileged EXEC

show auto-copy-sw (for stack firmware synchronization)

M4350

Use this command to display the stack firmware synchronization configuration status.

Format	<code>show auto-copy-sw</code>
Mode	Privileged EXEC

Term	Definition
Synchronization	Shows whether the SFS feature is enabled.
SNMP Trap Status	Shows whether the stack sends traps for SFS events
Allow Downgrade	Shows whether the stack manager is permitted to downgrade the firmware version of a stack member.

Nonstop Forwarding Commands for Stack Configuration

You can describe a switch in terms of three semi-independent functions: 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 determines how the forwarding plane must forward packets, which data packets can be forwarded, and where the data packets must be forwarded to.

Application software on the management unit functions as the control plane. The management plane is also application software that runs on the management unit and that provides interfaces, allowing you to configure and monitor the device.

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.

You can also manually initiate a nonstop forwarding failover by issuing the **initiate failover** command. If the management unit fails, traffic flows that enter and exit the stack through physical ports on a unit other than the management unit continue with at most a subsecond interruption.

To prepare the backup management unit for a failover, applications on the management unit continuously checkpoint (that is, forward) 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 do not need 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 (that is, forwarded) information. While the control plane is initializing, the stack cannot react to external changes, such as network topology changes. When the control plane is fully operational on the new management unit, the control plane ensures that the hardware state is updated as necessary. The 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 protocol 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 (see [“IP Event Dampening Commands on page 1070”](#)).
- A protocol can simply restart after the failover if neighbors react slowly enough that they do not 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 configured over port channels that span two or more stack units and layer 3 routes must be configured over ECMP routes with next hops over 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.

nsf (Stack Global Config)

M4350

Use this command to enable nonstop forwarding on the stack. When nonstop forwarding is enabled, if the management unit of a stack fails, the backup unit takes over as the primary management unit without clearing the hardware tables of any of the surviving units. Data traffic continues to be forwarded in hardware while the management functions initialize on the backup unit.

NSF is enabled by default on platforms that support it. You can disable NSF to redirect the CPU resources that are consumed by data checkpointing (that is, data forwarding).

If a unit that does not support NSF is connected to the stack, NSF is disabled on all stack members. If a unit that does not support NSF is disconnected from the stack, all other units do support NSF, and NSF is administratively enabled, NSF operation resumes.

Default	Enabled
Format	<code>nsf</code>
Mode	Stack Global Config

`no nsf`

Use this command to disable nonstop forwarding on the stack.

Format	<code>no nsf</code>
Mode	Stack Global Config

`show nsf` (for stack configuration)

M4350

Use this command to display global and per-unit information for the nonstop forwarding configuration on the stack.

Format	<code>show nsf</code>
Mode	Privileged EXEC

Term	Definition
NSF Administrative Status	Indicates whether nonstop forwarding is administratively enabled or disabled. The default is Enabled.
NSF Operational Status	Indicates whether NSF is enabled on the stack.
Last Startup Reason	The type of activation that caused the software to start the last time: • “Power-On” means that the switch rebooted. A reboot can be caused by a power cycle or an administrative “Reload” command. • “Administrative Move” means that someone issued the <code>movemanagement</code> command for the stand-by manager to take over. • “Warm-Auto-Restart” means that the primary management card restarted because of a failure, and the system executed a nonstop forwarding failover. • “Cold-Auto-Restart” means that the system switched from the active manager to the backup manager and was unable to maintain user data traffic. This is usually caused by multiple failures occurring in a short period.
Time Since Last Restart Time	The time since the current management unit became the active management unit.

Term	Definition
Restart in progress	Indicates whether a restart is in progress.
Warm Restart Ready	Indicates whether the system is ready to perform a nonstop forwarding failover from the management unit to the backup unit.
Copy of Running Configuration to Backup Unit: Status	Indicates whether the running configuration on the backup unit includes all changes made on the management unit. Displays as Current or Stale.
Time Since Last Copy	The time when the running configuration was last copied from the management unit to the backup unit.
Time Until Next Copy	The number of seconds until the running configuration is copied to the backup unit. This line only appears when the running configuration on the backup unit is Stale.
NSF Support (<i>Per Unit Status Parameter</i>)	Indicates whether a unit supports NSF.

initiate failover (for stack configuration)

M4350

Use this command to force the backup unit to take over as the management unit and perform a “warm restart” of the stack. On a warm restart, the backup unit becomes the management unit without clearing its hardware tables (on a cold restart, hardware tables are cleared).

Applications apply checkpointed data (that is, forwarded data) from the former management unit. The original management unit reboots. If the system is not ready for a warm restart, for example because no backup unit was elected or one or more members of the stack do not support nonstop forwarding, the command fails with a warning message.

The **movemanagement** command (see [movemanagement \(Stack Global Config\)](#) on page 30) also transfers control from the current management unit. However, the hardware is cleared and all units reinitialize.

Default	None
Format	<code>initiate failover</code>
Mode	Stack Global Config

show checkpoint statistics (for stack configuration)

M4350

Use this command to display general information about the checkpoint service operation.

Format	<code>show checkpoint statistics</code>
Mode	Privileged EXEC

Term	Description
Messages Checkpointed	The number of checkpoint messages that are transmitted to the backup unit. Range: Integer. Default: 0
Bytes Checkpointed	The number of bytes transmitted to the backup unit. Range: Integer. Default: 0
Time Since Counters Cleared	The number of days, hours, minutes and seconds since the counters were reset to zero. The counters are cleared when a unit becomes manager or when you issue the clear checkpoint statistics command. Range: Time Stamp. Default: 0d00:00:00
Checkpoint Message Rate Average	The average number of checkpoint messages per second. The average is computed over the period since the counters were cleared. Range: Integer. Default: 0
Last 10-second Message Rate Average	The average number of checkpoint messages per second in the last 10-second interval. This average is updated once every 10 seconds. Range: Integer. Default: 0
Highest 10-second Message Rate	The highest rate recorded over a 10-second interval since the counters were cleared. Range: Integer. Default: 0

Command example:

```
(Switch)#show checkpoint statistics
Messages Checkpointed.....6708
Bytes Checkpointed.....894305
Time Since Counters Cleared.....3d 01:05:09
Checkpoint Message Rate Average.....0.025 msg/sec
Last 10-second Message Rate Average.....0 msg/sec
Highest 10-second Message Rate.....8 msg/sec
```

clear checkpoint statistics (for stack configuration)

M4350

Use this command to clear the statistics for the checkpointing process.

Format	clear checkpoint statistics
Mode	Privileged EXEC

5

Management Commands

This chapter describes the management commands.

The chapter contains the following sections:

- [Configure the Switch Management CPU](#)
- [CPU Queue Commands](#)
- [Management Interface Commands](#)
- [IPv6 Management Commands](#)
- [Console Port Access Commands](#)
- [Telnet Commands](#)
- [Secure Shell Commands](#)
- [Management Security Commands](#)
- [Management Access Control List Commands](#)
- [Hypertext Transfer Protocol Commands](#)
- [Access Commands](#)
- [User Account Commands](#)
- [SNMP Commands](#)
- [RADIUS Commands](#)
- [TACACS+ Commands](#)
- [Configuration Scripting Commands](#)
- [Prelogin Banner, System Prompt, and Host Name Commands](#)
- [Application Commands](#)
- [OpenFlow Commands](#)
- [Cloud Managed Commands](#)

The commands in this chapter are in one of three functional groups:

- **Show commands.** Display switch settings, statistics, and other information.
- **Configuration commands.** Configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- **Clear commands.** Clear some or all of the settings to factory defaults.

Configure the Switch Management CPU

To manage the switch over the web management interface or Telnet, you must assign an IP address to the switch management CPU. You can accomplish this task through CLI commands or you can use the ezconfig tool, which simplifies the task. The tool lets you configure the following settings:

- The administrator user password and administrator-enable password
- The management CPU IP address and network mask
- The system name and location information

The tool is interactive and uses questions to guide you through the configuration steps. At the end of the configuration session, the tool lets you save the information. To see which information was changed by the ezconfig tool after a configuration session, issue the **show running-config** command.

ezconfig

M4250

M4350

This command sets the IP address, subnet mask, and gateway of the switch. The IP address and the gateway must be on the same subnet.

Format	ezconfig
Mode	Privileged EXEC

```

(NETGEAR Switch) #ezconfig

EZ Configuration Utility
-----
Hello and Welcome!
This utility will walk you thru assigning the IP address for the switch
management CPU. It will allow you to save the changes at the end. After
the session, simply use the newly assigned IP address to access the Web
GUI using any public domain Web browser.

Admin password is not defined.
Do you want to assign the admin password (password length must be in range of 8-64
characters) (Y/N/Q)? y

Enter new password:*****
Confirm new password:*****

The 'enable' password required for switch configuration via the command
line interface is currently not configured.
```

Fully Managed Switches M4250 and M4350 Series

Do you want to assign it (password length must be in range of 8-64 characters) (Y/N/Q)?
y

Enter new password:*****

Confirm new password:*****

Current IPv4 Management Interface: vlan 1

Do you want to set new Management VLAN ID (Y/N/Q)?y

VLAN ID: 1

Assigning an IPv4 address to your switch management

Current IPv4 Address Configuration

Management VLAN ID: vlan 1

IPv4 Address Assignment Mode: None

IPv4 Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

Routing Mode: Enable

IPv4 address is not assigned. What do you want to do?

C - Configure IPv4 address manually.

D - Assign IPv4 address for the switch using DHCP Mode(current IPv4 address will be lost).

N - Skip this option and go to the next question.

Q - Quit.

? - Help.

(C/D/N/Q/?)? c

IPv4 Address: 192.168.1.1

Network Mask: 255.255.255.0

Gateway: 192.168.254

Incorrect input! Gateway must be a valid IP address.

Try again (Y/N/Q)? y

Gateway: 192.168.1.254

Do you want to enable global routing (Y/N)?y

Current IPv6 Management Interface: (not configured)

Do you want to set new IPv6 Management VLAN ID (Y/N/Q)?y

VLAN ID: 1

Assigning management IPv6 address.

Current IPv6 Address Configuration

IPv6 Address: fe80::abd:43ff:fe71:73c0/64

IPv6 Current state: TENT

Fully Managed Switches M4250 and M4350 Series

Address DHCP Mode: Disabled

Address Autoconfigure Mode: Disabled

EUI64 : Enabled

Routing Mode: Enable

IPv6 address has been assigned manually. What do you want to do?

C - Add IPv6 address.

D - Assign IPv6 address for the switch using DHCP Mode.

A - Assign IPv6 address for the switch using Auto Mode.

N - Skip this option and go to the next question.

Q - Quit.

? - Help.

(C/D/A/N/Q/?)? c

IPv6 Address: 2001:1::1

IPv6 Prefix-length: 64

IPv6 EUI64 flag (Y/N): n

IPv6 Gateway: 2001:1::fffe

Current Out of Band(service port) IPv4 Address Configuration

IP Address Assignment Mode: DHCP

IP Address: 172.26.2.104

Subnet Mask: 255.255.255.0

Default Router: 172.26.2.1

IPv4 address will be assigned automatically by the DHCP server in your network. You can disable DHCP mode and use static(fixed) IPv4 address. If fixed IPv4 Address Mode is selected, DHCP Protocol Mode will be disabled, and you will be prompted to set the values for the four fields above.

Do you want to assign IPv4 address manually? (Y/N/Q/?) y

IPv4 Address: 172.26.2.1

Network Mask: 255.255.255.0

Gateway: 172.26.2.254

Current Out of Band(Serviceport) IPv6 Address Configuration

Service port IPv6 Address Mode: None

IPv6 Administrative Mode: Enabled

Service port IPv6 Address Mode autoconfigure: Disabled

IPv6 Address: fe80::abd:43ff:fe71:73be/64

Service port IPv6 address gateway:

EUI Flag: False

Fully Managed Switches M4250 and M4350 Series

IPv6 address has been assigned manually. What do you want to do?

A - Assign IPv6 address for the switch using Auto Mode.

D - Assign IPv6 address for the switch using DHCP Mode.

G - Assign IPv6 Gateway.

C - Add IPv6 address.

N - Skip this option and go to the next question.

Q - Quit.

? - Help.

(A/D/G/C/N/Q/?)? c

Current Management Interface Configuration

Management Interface: L3 Management VLAN

Current management interface is L3 Management VLAN. What do you want to do?

O - Change to Out of Band port(service port).

V - Change to L3 Management VLAN.

N - Skip this option and go to the next question.

Q - Quit.

? - Help.

(O/V/N/Q/?)?n

Assigning System Name, System Location and System Contact to your switch management

Current Configuration

System Name:

System Location:

System Contact:

Do you want to assign switch name and location information? (Y/N/Q)

CPU Queue Commands

You can send all packets with a specified destination address to a higher priority queue (5) than the default queue for data packets and unicast packets to the CPU.

`ip cpu-priority`

M4250

M4350

This command sends all packets with a specified destination IPv4 address to a higher priority queue (5) than the default queue for data packets and unicast packets to the CPU.

Format	<code>ip cpu-priority ip-address</code>
Mode	Global Config

`no ip cpu-priority`

This command removes all packets with a specified destination IPv4 address from the higher priority queue.

Format	<code>no ip cpu-priority ip-address</code>
Mode	Global Config

`ipv6 cpu-priority`

M4250

M4350

The command allows all packets with a specified destination IPv6 address into a higher priority queue (5) than the default queue for data packets and unicast packets to the CPU.

Format	<code>ip cpu-priority ipv6-address</code>
Mode	Global Config

`no ipv6 cpu-priority`

This command removes all packets with a specified destination IPv6 address from the higher priority queue.

Format	<code>no ip cpu-priority ipv6-address</code>
Mode	Global Config

Management Interface Commands

This section describes the commands you use to configure a logical IPv4 interface for management access.

enable (Privileged EXEC access)

M4250

M4350

This command gives you access to the Privileged EXEC mode. From the Privileged EXEC mode, you can configure the network interface.

Format	enable
Mode	User EXEC

do (Privileged EXEC commands)

M4250

M4350

This command executes Privileged EXEC mode commands from any of the configuration modes.

Format	do <i>Priv Exec Mode Command</i>
Mode	• Global Config • Interface Config • VLAN Config (also referred to as VLAN Database) • Routing Config

Command example:

The following is an example of the **do** command that executes the Privileged Exec command **script list** in Global Config Mode.

```
(NETGEAR Switch) #configure
(NETGEAR Switch) (config)#do script list
```

Configuration Script Name	Size(Bytes)
-----	-----
backup-config	2105
running-config	4483
startup-config	445

```
3 configuration script(s) found.
2041 Kbytes free.
```

ip management

M4250

M4350

Use this command to create an IPv4 management interface, enable DHCP on the IPv4 management interface, delete a previous IPv4 management interface, and set the source interface for all applications, including RADIUS, TACACS, DNS, SNTP, SNMP, and SysLog.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Default	vlan 1
Format	ip management {vlan number port unit/port} {dhcp ipaddr {prefix-length subnet-mask}}
Mode	Global Config

ip management source-interface

M4250

M4350

Use this command to specify the source IP address for all applications, including RADIUS, TACACS, DNS, SNTP, SNMP, and SysLog.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

For the **loopback** keyword, you can enter a number between 0 and 7.

Default	vlan 1
Format	ip management source-interface {serviceport vlan number port unit/slot/port loopback number}
Mode	Global Config

no ip management

Use this command to reset the IPv4 management interface to the default settings.

Format	no ip management
Mode	Global Config

serviceport ip

M4250

M4350

This command sets the IP address, the netmask, and the gateway of the network management port. You can specify the **none** option to clear the IPv4 address and mask and the default gateway (that is, reset each of these values to 0.0.0.0).

Format	<code>serviceport ip {ipaddr netmask [gateway] none}</code>
Mode	Privileged EXEC

serviceport protocol

M4250

M4350

This command specifies the network management port configuration protocol. If you modify this value, the change is effective immediately. If you use the **bootp** parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the **dhcp** parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the **none** parameter, you must configure the network information for the switch manually.

Format	<code>serviceport protocol {none bootp dhcp}</code>
Mode	Privileged EXEC

serviceport protocol dhcp

M4250

M4350

This command enables the DHCPv4 client on a service port. If you use the **client-id** optional parameter, the DHCP client messages are sent with the client identifier option.

Default	none
Format	<code>serviceport protocol dhcp [client-id]</code>
Mode	Privileged Exec

There is no support for the **no** form of the command **serviceport protocol dhcp client-id**. To remove the **client-id** option from the DHCP client messages, issue the command **serviceport protocol dhcp** without the **client-id** option. The command **serviceport protocol none** can be used to disable the DHCP client and client-id option on the interface.

Command example:

```
(NETGEAR Switch) # serviceport protocol dhcp client-id
```

mac management address

M4250

M4350

This command sets locally administered MAC addresses. The following rules apply:

- Bit 6 of byte 0 (called the U/L bit) indicates whether the address is universally administered (b'0') or locally administered (b'1').
- Bit 7 of byte 0 (called the I/G bit) indicates whether the destination address is an individual address (b'0') or a group address (b'1').
- The second character, of the twelve character macaddr, must be 2, 6, A or E.

A locally administered address must have bit 6 On (b'1') and bit 7 Off (b'0').

Format	mac management address <i>macaddr</i>

Mode	Privileged EXEC

mac management type

M4250

M4350

This command specifies whether the switch uses the burned in MAC address or the locally-administered MAC address.

Default	burnedin

Format	mac management type {local burnedin}

Mode	Privileged EXEC

no network mac-type

This command resets the value of MAC address to its default.

Format	no mac management type

Mode	Privileged EXEC

show ip management

M4250

M4350

This command displays configuration settings that are associated with the switch management interface. The management interface is the logical interface that is used for in-band connectivity with the switch over any of the switch front panel ports. The configuration parameters that are associated with the switch management interface do not affect the configuration of the front panel ports through which traffic is switched or routed. The management interface is always considered to be up, whether or not any member ports are up. Therefore, the output of the **show ip management** command always shows interface status as up.

Format	show ip management
Modes	- Privileged EXEC - User EXEC
Term	Definition
Interface Status	The management interface status; it is always considered to be up.
IP Address	The IP address of the interface. The factory default value is 0.0.0.0.
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0.
IPv6 Administrative Mode	Whether enabled or disabled.
IPv6 Address/Length	The IPv6 address and length.
IPv6 Default Router	The IPv6 default router address.
Burned In MAC Address	The burned- in MAC address used for in-band connectivity.
Locally Administered MAC Address	You can configure a locally administered MAC address for in-band connectivity. This configuration requires the following: - The MAC Address Type must be set to Locally Administered. - Enter the address as 12 hexadecimal digits (6 bytes) with a colon between bytes. - Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0. That is, byte 0 must contain the xxxx xx10 mask. - The MAC address must be unique. We recommend that you use the MAC address that is the numerically smallest MAC address of all ports that belong to the bridge. When concatenated with dot1dStpPriority, a unique Bridge Identifier is formed, which is used in the Spanning Tree Protocol.
MAC Address Type	The MAC address that must be used for in-band connectivity. The choices are the burned in or the Locally Administered address. The factory default is to use the burned in MAC address.
DHCPv6 Client DUID	The DHCPv6 client's unique client identifier. This row is displayed only when the configured IPv6 protocol is DHCP.

Term	Definition
IPv6 Autoconfig Mode	Whether IPv6 Stateless address autoconfiguration is enabled or disabled.
DHCP Client Identifier	The client identifier is displayed in the output of the command only if DHCP is enabled with the client-id option on the management interface.

Command example:

```
(NETGEAR Switch) #show ip management
```

```
IPv4 Interface Status..... Up
IPv4 Management Interface..... vlan 1
IP Address..... 169.254.100.100
Subnet Mask..... 255.255.255.0
Method..... DHCP
Routing Mode..... Enable
Default Gateway..... 0.0.0.0

Source Interface..... vlan 1
Burned In MAC Address..... DC:EF:09:D3:2D:48
Locally Administered MAC address..... 00:00:00:00:00:00
MAC Address Type..... Burned In
```

```
IPv6 Management Interface is not Configured.
```

show serviceport**M4250****M4350**

This command displays service port configuration information.

Format	show serviceport

Mode	- Privileged EXEC - User EXEC

Term	Definition
Interface Status	The network interface status. It is always considered to be up.
IP Address	The IP address of the interface. The factory default value is 0.0.0.0.
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0.
IPv6 Administrative Mode	Whether enabled or disabled. Default value is enabled.
IPv6 Address/Length	The IPv6 address and length. Default is Link Local format.

Term	Definition
IPv6 Default Router	The IPv6 default router address on the service port. The factory default value is an unspecified address.
Configured IPv4 Protocol	The IPv4 network protocol being used. The options are bootp dhcp none.
Configured IPv6 Protocol	The IPv6 network protocol being used. The options are dhcp none.
DHCPv6 Client DUID	The DHCPv6 client's unique client identifier. This row is displayed only when the configured IPv6 protocol is dhcp.
IPv6 Autoconfig Mode	Whether IPv6 Stateless address autoconfiguration is enabled or disabled.
Burned in MAC Address	The burned in MAC address used for in-band connectivity.
DHCP Client Identifier	The client identifier is displayed in the output of the command only if DHCP is enabled with the client-id option on the service port.

Command example:

The following example displays output for the service port:

```
(Netgear switch) #show serviceport
```

```
Interface Status..... Up
IP Address..... 10.230.3.51
Subnet Mask..... 255.255.255.0
Default Gateway..... 10.230.3.1
IPv6 Administrative Mode..... Enabled
IPv6 Prefix is ..... fe80::210:18ff:fe82:640/64
IPv6 Prefix is ..... 2005::21/128
IPv6 Default Router is ..... fe80::204:76ff:fe73:423a
Configured IPv4 Protocol ..... DHCP
Configured IPv6 Protocol ..... DHCP
DHCPv6 Client DUID ..... 00:03:00:06:00:10:18:82:06:4C
IPv6 Autoconfig Mode..... Disabled
Burned In MAC Address..... 00:10:18:82:06:4D
DHCP Client Identifier..... 0NETGEAR-0010.1882.160C
```

IPv6 Management Commands

IPv6 management commands allow a device to be managed via an IPv6 address in a switch or through IPv4 routing (that is, independent from the IPv6 routing package). For Routing/IPv6 builds of the switch software, dual IPv4/IPv6 operation over the service port is enabled. The switch software provides capabilities such as the following”

- Static assignment of IPv6 addresses and gateways for the service/network ports.
- The ability to ping an IPv6 link-local address over the service/network port.
- Using IPv6 management commands, you can send SNMP traps and queries via the service/network port.
- The user can manage a device via the network port (in addition to a Routing Interface or the Service port).

ipv6 management

M4250

M4350

Use this command to create an IPv6 management interface, enable IPv6 and DHCPv6 on the management interface, and delete a previous IPv6 management interface, if there was any. (The switch does not provide a default IPv6 management interface.)

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>ipv6 management {vlan number port unit/slot/port} {autoconfig dhcp prefix prefix-length}</code>
Mode	Global Config

no ipv6 management

Use this command to reset the IPv6 management interface to the default settings, that is, remove the IPv6 management interface. (The switch does not provide a default IPv6 management interface.)

Format	<code>no ipv6 management</code>
Mode	Global Config

serviceport ipv6 enable

M4250

M4350

Use this command to enable IPv6 operation on the service port. By default, IPv6 operation is enabled on the service port.

Default	enabled
Format	serviceport ipv6 enable
Mode	Privileged EXEC

no serviceport ipv6 enable

Use this command to disable IPv6 operation on the service port.

Format	no serviceport ipv6 enable
Mode	Privileged EXEC

serviceport ipv6 address

M4250

M4350

Use the options of this command to manually configure IPv6 global address, enable/disable stateless global address autoconfiguration and to enable/disable dhcpv6 client protocol information on the service port.

Note: Multiple IPv6 prefixes can be configured on the service port.

no serviceport ipv6 address

Use the command **no serviceport ipv6 address** to remove all configured IPv6 prefixes on the service port interface.

Use the command with the address option to remove the manually configured IPv6 global address on the network port interface.

Use the command with the autoconfig option to disable the stateless global address autoconfiguration on the service port.

Use the command with the dhcp option to disable the dhcpv6 client protocol on the service port.

Format	<code>no serviceport ipv6 address {address/prefix-length [eui64] autoconfig dhcp}</code>

Mode	Privileged EXEC

serviceport ipv6 gateway

M4250

M4350

Use this command to configure IPv6 gateway information (that is, default router information) for the service port.

Note: Only a single IPv6 gateway address can be configured for the service port. There might be a combination of IPv6 prefixes and gateways that are explicitly configured and those that are set through auto-address configuration with a connected IPv6 router on its service port interface.

Format	<code>serviceport ipv6 gateway gateway-address</code>

Mode	Privileged EXEC

Parameter	Description

gateway-address	Gateway address in IPv6 global or link-local address format.

no serviceport ipv6 gateway

Use this command to remove IPv6 gateways on the service port interface.

Format	<code>no serviceport ipv6 gateway</code>

Mode	Privileged EXEC

serviceport ipv6 neighbor

M4250

M4350

Use this command to manually add IPv6 neighbors to the IPv6 neighbor table for the service port. If an IPv6 neighbor already exists in the neighbor table, the entry is automatically converted to a static entry. Static entries are not modified by the neighbor discovery process.

They are, however, treated the same for IPv6 forwarding. Static IPv6 neighbor entries are applied to the hardware when the corresponding interface is operationally active.

Format	<code>serviceport ipv6 neighbor ipv6-address macaddr</code>

Mode	Privileged EXEC

Parameter	Description

ipv6-address	The IPv6 address of the neighbor or interface.

macaddr	The link-layer address.

`no serviceport ipv6 neighbor`

Use this command to remove IPv6 neighbors from the IPv6 neighbor table for the service port.

Format	<code>no serviceport ipv6 neighbor ipv6-address macaddr</code>

Mode	Privileged EXEC

`show serviceport ipv6 neighbors`

M4250

M4350

Use this command to displays information about the IPv6 neighbor entries cached on the service port. The information is updated to show the type of the entry.

Default	None

Format	<code>show serviceport ipv6 neighbors</code>

Mode	Privileged EXEC

Field	Description

IPv6 Address	The IPv6 address of the neighbor.

MAC Address	The MAC Address of the neighbor.

isRtr	Shows if the neighbor is a router. If TRUE, the neighbor is a router; if FALSE, it is not a router.

Neighbor State	The state of the neighbor cache entry. The possible values are: Incomplete, Reachable, Stale, Delay, Probe, and Unknown.

Age	The time in seconds that has elapsed since an entry was added to the cache.

Type	The type of neighbor entry. The type is Static if the entry is manually configured and Dynamic if dynamically resolved.

Command example:

```
(NETGEAR Switch) #show serviceport ipv6 neighbors
```

IPv6 Address	MAC Address	isRtr	Neighbor State	Age (Secs)	Type
FE80::5E26:AFF:FEBD:852C	5c:26:0a:bd:85:2c	FALSE	Reachable	0	Dynamic

ping ipv6

M4250

M4350

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI and Web interfaces. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. Use the *ipv6-address* or *hostname* parameter to ping an interface by using the global IPv6 address of the interface.

The interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

You can utilize the ping or traceroute facilities over the service or network ports when using an IPv6 global address *ipv6-global-address* or *hostname*. Any IPv6 global address or gateway assignments to these interfaces causes IPv6 routes to be installed such that the ping or traceroute request is routed out the service or network port properly. When referencing an IPv6 link-local address, you must specify the **interface** keyword with either the *unit/slot/port* argument, **vlan** keyword and *vlan-id* argument, or **serviceport** keyword.

Use the optional **size** keyword and *datagram-size* parameter to specify the size of the ping packet.

Default	The default count is 1.
	The default interval is 3 seconds.
	The default size is 0 bytes.

Format	<code>ping ipv6 {ipv6-global-address hostname {interface {unit/slot/port vlan vlan-id serviceport} link-local-address} [size datagram-size]}</code>
Mode	Privileged EXEC User Exec

ping ipv6 interface

M4250

M4350

Use this command to determine whether another computer is on the network. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. You can use a loopback, network port, service port, VLAN, or physical interface as the source.

The interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093. Use the optional **size** keyword and *datagram-size* parameter to specify the size of the ping packet.

Format	<code>ping ipv6 interface {unit/slot/port vlan vlan-id loopback loopback-id serviceport} {link-local-address link-local-address ipv6-address} [size datagram-size]</code>
Modes	Privileged EXEC User Exec

Console Port Access Commands

This section describes the commands you use to configure the console port. You can use a serial cable to connect a management host directly to the console port of the switch.

configure (or config)

M4250

M4350

This command gives you access to the Global Config mode. You can also enter the abbreviated **confi****g**. From the Global Config mode, you can configure a variety of system settings, including user accounts. From the Global Config mode, you can enter other command modes, including the Line Config, SSH Config, and Telnet Config modes.

Format	configure
Mode	Privileged EXEC

line console

M4250

M4350

This command gives you access to the Line Config mode (Config-line), which allows you to configure console port settings, and various SSH and Telnet settings. You can also configure console login and enable authentication.

Note: After you enter Line Config mode, you can use most commands in that mode not only for a console connection, but also for an SSH and Telnet connection.

Format	line console
Mode	Global Config

Command example:

```
((NETGEAR Switch) (config) #line console
(NETGEAR Switch) (Config-line) #
```


serial baudrate (Line Config)

M4250**M4350**

This command specifies the communication rate of the terminal interface for a console connection. The supported rates are 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Default	9600
Format	<code>serial baudrate {1200 2400 4800 9600 19200 38400 57600 115200}</code>
Mode	Line Config

no serial baudrate (Line Config)

This command sets the communication rate of the terminal interface for a console connection.

Format	<code>no serial baudrate</code>
Mode	Line Config

serial timeout (Line Config)

M4250**M4350**

This command specifies the maximum connect time (in minutes) without console activity. A value of 0 indicates that a console can be connected indefinitely. The time range is 0 to 160.

Default	5
Format	<code>serial timeout 0-160</code>
Mode	Line Config

no serial timeout (Line Config)

This command sets the maximum connect time (in minutes) without console activity.

Format	<code>no serial timeout</code>
Mode	Line Config

set sup-console

M4350

On an M4350 series switch, this command allows access to the full CLI from any stack member. By default, the primary management unit is allowed full CLI access. You can move full CLI access among the stack members, but at any time, only one stack member can

access the management CLI. You can issue the command on the stack member or backup unit. After the console is transferred to the backup unit or to a stack member unit, access to the full CLI on the primary management unit is disabled to avoid multiple simultaneous CLI inputs. You can restore full access on the primary management unit by entering the command on the serial port of the primary management unit.

Note: If you enter the command while the primary management unit is already allowed full CLI access, the command does not take effect.

Format	<code>set sup-console</code>

Mode	Privileged EXEC

show serial

M4250

M4350

This command displays serial communication settings for the switch.

Format	<code>show serial</code>

Modes	- Privileged EXEC - User EXEC

Term	Definition
Serial Port Login Timeout (minutes)	The time, in minutes, of inactivity on a serial port connection, after which the switch will close the connection. A value of 0 disables the timeout.
Baud Rate (bps)	The default baud rate at which the serial port will try to connect.
Character Size (bits)	The number of bits in a character. The number of bits is always 8.
Flow Control	Whether Hardware Flow-Control is enabled or disabled. Hardware Flow Control is always disabled.
Stop Bits	The number of Stop bits per character. The number of Stop bits is always 1.
Parity	The parity method used on the Serial Port. The Parity Method is always None.

Telnet Commands

This section describes the commands you use to configure and view Telnet settings. You can use Telnet to manage the device from a remote management host.

ip telnet server enable

M4250

M4350

Use this command to enable Telnet connections to the system and to enable the Telnet Server Admin Mode. This command opens the Telnet listening port.

Default	enabled
Format	ip telnet server enable
Mode	Privileged EXEC

no ip telnet server enable

Use this command to disable Telnet access to the system and to disable the Telnet Server Admin Mode. This command closes the Telnet listening port and disconnects all open Telnet sessions.

Format	no ip telnet server enable
Mode	Privileged EXEC

ip telnet port

M4250

M4350

Use this command to configure the TCP port number on which the Telnet server detects requests. The *number* argument can be a port number in the range from 1 to 65535.

Default	23
Format	ip telnet port <i>number</i>
Mode	Privileged EXEC

no ip telnet port

Use this command to reset the TCP port number on which the Telnet server detects requests to the default of 23.

Format	no ip telnet port
Mode	Privileged EXEC

telnet

M4250

M4350

This command establishes a new outbound Telnet connection to a remote host. The host must be a valid IP address or host name. Valid values for *port* should be a valid decimal integer in the range of 0 to 65535, where the default value is 23. If **debug** is used, the current Telnet options enabled is displayed. The optional **line** parameter sets the outbound Telnet operational mode as linemode where, by default, the operational mode is character mode. The **localecho** option enables local echo.

Format	telnet { <i>ip-address</i> <i>hostname</i> } <i>port</i> [debug] [line] [localecho]
Modes	- Privileged EXEC - User EXEC

transport input telnet (Line Config)

M4250

M4350

This command regulates new Telnet sessions. If enabled, new Telnet sessions can be established until there are no more sessions available. An established session remains active until the session is ended or an abnormal network error ends the session.

Access the Line Config mode by entering the **line console** command in Global Config mode.

Note: If the Telnet Server Admin Mode is disabled, Telnet sessions cannot be established. Use the **ip telnet server enable** command to enable Telnet Server Admin Mode.

Default	enabled
Format	transport input telnet
Mode	Line Config

no transport input telnet (Line Config)

Use this command to prevent new Telnet sessions from being established.

Format	no transport input telnet

Mode	Line Config

transport output telnet (Line Config)

M4250

M4350

This command regulates new outbound Telnet connections. If enabled, new outbound Telnet sessions can be established until the system reaches the maximum number of simultaneous outbound Telnet sessions allowed. An established session remains active until the session is ended or an abnormal network error ends it.

Access the Line Config mode by entering the **line console** command in Global Config mode.

Default	enabled

Format	transport output telnet

Mode	Line Config

no transport output telnet (Line Config)

Use this command to prevent new outbound Telnet connection from being established.

Format	no transport output telnet

Mode	Line Config

session-limit (Line Config)

M4250

M4350

This command specifies the maximum number of simultaneous outbound Telnet sessions. The *number* argument can be a number in the range from 0–5. A value of 0 indicates that no outbound Telnet session can be established.

Access the Line Config mode by entering the **line console** command in Global Config mode.

Default	5

Format	session-limit <i>number</i>

Mode	Line Config

no session-limit (Line Config)

This command sets the maximum number of simultaneous outbound Telnet sessions to the default value.

Format	no session-limit

Mode	Line Config

session-timeout (Line Config)

M4250

M4350

This command sets the Telnet session time-out value. The time-out value unit of time is minutes and is specified by the *minutes* argument in the range 1–160 minutes.

Access the Line Config mode by entering the **line console** command in Global Config mode.

Default	5

Format	session-timeout <i>minutes</i>

Mode	Line Config

no session-timeout (Line Config)

This command sets the Telnet session time-out value to the default. The time-out value unit of time is minutes.

Format	no session-timeout

Mode	Line Config

telnetcon maxsessions

M4250

M4350

This command specifies the maximum number of Telnet connection sessions that can be established. The *number* argument can be a number in the range from 0–5. A value of 0 indicates that no Telnet connection can be established.

Default	5

Format	telnetcon maxsessions <i>number</i>

Mode	Privileged EXEC

no telnetcon maxsessions

This command sets the maximum number of Telnet connection sessions that can be established to the default value.

Format	no telnetcon maxsessions

Mode	Privileged EXEC

telnetcon timeout

M4250

M4350

This command sets the Telnet connection session time-out value. A session is active as long as the session has not been idle for the value set. The time-out value unit of time is minutes and is specified by the *minutes* argument in the range 1–160 minutes.

Note: When you change the time-out value, the new value is applied to all active and inactive sessions immediately. Any sessions that have been idle longer than the new time-out value are disconnected immediately.

Default	5

Format	telnetcon timeout <i>minutes</i>

Mode	Privileged EXEC

no telnetcon timeout

This command sets the Telnet connection session timeout value to the default.

Note: Changing the time-out value for active sessions does not become effective until the session is accessed again. Also, any keystroke activates the new time-out duration.

Format	no telnetcon timeout

Mode	Privileged EXEC

line telnet

M4250**M4350**

This command gives you access to the Telnet Config mode (Config-telnet) for a virtual terminal for remote console access (Telnet). This mode lets you configure the Telnet settings.

Format	line telnet
Mode	Global Config

Command example:

```
(NETGEAR Switch) (config)#line telnet
(NETGEAR Switch) (config-telnet)#
```

show telnet

M4250**M4350**

This command displays the current outbound Telnet settings. In other words, these settings apply to Telnet connections initiated from the switch to a remote system.

Format	show telnet
Modes	- Privileged EXEC - User EXEC

Term	Definition
Outbound Telnet Login Timeout	The number of minutes an outbound Telnet session is allowed to remain inactive before being logged off.
Maximum Number of Outbound Telnet Sessions	The number of simultaneous outbound Telnet connections allowed.
Allow New Outbound Telnet Sessions	Indicates whether outbound Telnet sessions will be allowed.

show telnetcon

M4250

M4350

This command displays the current inbound Telnet settings. In other words, these settings apply to Telnet connections initiated from a remote system to the switch.

Format	show telnetcon
Modes	- Privileged EXEC - User EXEC
Term	Definition
Remote Connection Login Timeout (minutes)	This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. May be specified as a number from 1 to 160. The factory default is 5.
Maximum Number of Remote Connection Sessions	This object indicates the number of simultaneous remote connection sessions allowed. The factory default is 5.
Allow New Telnet Sessions	New Telnet sessions will not be allowed when this field is set to no. The factory default value is yes.
Telnet Server Admin Mode	States whether the Telnet Server Admin Mode is enabled or disabled.
Telnet Server Port	The port number on which the Telnet server can detect requests.

Secure Shell Commands

This section describes the commands you use to configure Secure Shell (SSH) access to the switch. Use SSH to access the switch from a remote management host. The switch allows a maximum of 5 SSH sessions.

ip ssh

M4250

M4350

Use this command to enable SSH access to the system. (This command is the short form of the **ip ssh server enable** command.)

Default	disabled
Format	ip ssh
Mode	Privileged EXEC

no ip ssh

This command disables the IP secure shell server. (This command is the short form of the **no ip ssh server enable** command.)

Format	no ip ssh
Mode	Privileged EXEC

ip ssh server enable

M4250

M4350

This command enables the IP secure shell server.

Default	enabled
Format	ip ssh server enable
Mode	Privileged EXEC

no ip ssh server enable

This command disables the IP secure shell server. No new SSH connections are allowed, but the existing SSH connections continue to work until timed-out or logged-out.

Format	no ip ssh server enable
Mode	Privileged EXEC

ip ssh port

M4250

M4350

Use this command to configure the TCP port number on which the Secure Shell (SSH) server detects requests. The *number* argument can be a port number in the range from 1 to 65535.

Default	22
Format	ip ssh port <i>number</i>
Mode	Privileged EXEC

no ip ssh port

Use this command to reset the TCP port number on which the SSH server detects requests to the default of 22.

Format	no ip ssh port
Mode	Privileged EXEC

ip ssh pubkey-auth

M4250

M4350

Use this command to enable public key authentication for incoming SSH sessions.

Default	Disabled
Format	ip ssh pubkey-auth
Mode	Privileged EXEC

no ip ssh pubkey-auth

Use this command to disable public key authentication, which prevents SSH access to the switch.

Format	no ip ssh pubkey-auth
Mode	Privileged EXEC

sshcon maxsessions

M4250

M4350

This command specifies the maximum number of SSH connection sessions that can be established. The *number* argument can be a number in the range from 0–5. A value of 0 indicates that no SSH connection can be established. The range is 0 to 5.

Default	5
Format	sshcon maxsessions <i>number</i>
Mode	Privileged EXEC

no sshcon maxsessions

This command sets the maximum number of allowed SSH connection sessions to the default value.

Format	no sshcon maxsessions
Mode	Privileged EXEC

sshcon timeout

M4250

M4350

This command sets the SSH connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set. The time-out value unit of time is minutes and is specified by the *minutes* argument in the range 1–160 minutes.

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new time-out duration.

Default	5
Format	sshcon timeout <i>minutes</i>
Mode	Privileged EXEC

no sshcon timeout

This command sets the SSH connection session time-out value, in minutes, to the default.

Changing the time-out value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new time-out duration.

Format	no sshcon timeout
Mode	Privileged EXEC

ip ssh authentication-retries

M4250

M4350

Use this command to specify the maximum number of authentication retries allowed per SSH connection. You can set from 0 to 5 retries.

Default	3
Format	ip ssh authentication-retries {0-5}
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #ip ssh authentication-retries 2
```

```
no ip ssh authentication-retries
```

This command sets the maximum number of the maximum number of authentication retries to the default value.

Format	no ip ssh authentication-retries

Mode	Privileged EXEC

```
ip ssh server algorithm encryption
```

M4250

M4350

Use this command to specify the encryption algorithms used to establish the SSH connection. You must make at least one selection. If you select more than one option, the command defines the order of the encryption algorithms.

Default	All encryption algorithms are enabled by default.

Format	ip ssh server algorithm encryption {[aes128-ctr] [aes192-ctr] [aes256-ctr]}

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #ip ssh server algorithm encryption aes128-ctr aes192-ctr
```

```
no ip ssh server algorithm encryption
```

Use this command to disable the encryption algorithm.

Format	no ip ssh server algorithm encryption {[aes128-ctr] [aes192-ctr] [aes256-ctr]}

Mode	Privileged EXEC

ip ssh server algorithm hostkey

M4250**M4350**

Use this command to specify the host key algorithms used to establish the SSH connection. You must make at least one selection. If you select more than one option, the command defines the order of host key algorithms.

Default	All hostkey algorithms are enabled by default.
Format	<code>ip ssh server algorithm hostkey {[ssh-rsa] [rsa-sha2-256] [rsa-sha2-512] [ecdsa-sha2-nistp256] [ecdsa-sha2-nistp384] [ecdsa-sha2-nistp521]}</code>
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #ip ssh server algorithm hostkey ssh-rsa ecdsa-sha2-nistp384
```

no ip ssh server algorithm hostkey

Use this command to disable the host key algorithm.

Format	<code>no ip ssh server algorithm hostkey {[ssh-rsa] [rsa-sha2-256] [rsa-sha2-512] [ecdsa-sha2-nistp256] [ecdsa-sha2-nistp384] [ecdsa-sha2-nistp521]}</code>
Mode	Privileged EXEC

ip ssh server algorithm mac

M4250**M4350**

Use this command to specify the Message Authentication Code algorithms used to establish the SSH connection. You must make at least one selection. If you select more than one option, the command defines the order of the MAC algorithms.

Default	All mac algorithms are enabled by default.
Format	<code>ip ssh server algorithm mac {[hmac-sha2-256] [hmac-sha2-256-etm@openssh.com] [hmac-sha2-512] [hmac-sha2-512-etm@openssh.com]}</code>
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #ip ssh server algorithm mac hmac-md5-etm@openssh.com hmac-sha2-256
hmac-sha1
```

no ip ssh server algorithm mac

Use this command to disable the mac algorithm.

Format	no ip ssh server algorithm mac {[hmac-sha2-256] [hmac-sha2-256-etm@openssh.com] [hmac-sha2-512] [hmac-sha2-512-etm@openssh.com] }

Mode	Privileged EXEC

ip ssh server algorithm kex

M4250

M4350

Use this command to specify the key exchange (Kex) algorithms used to establish the SSH connection. You must make at least one selection. If you select more than one option, the command defines the order of the Kex algorithms.

Default	All Kex algorithms are enabled by default.

Format	ip ssh server algorithm kex {[curve25519-sha256] [curve25519-sha256@libssh.org] [diffie-hellman-group-exchange-sha256] [diffie-hellman-group14-sha1] [diffie-hellman-group14-sha256] [diffie-hellman-group16-sha512] [diffie-hellman-group18-sha512] [ecdh-sha2-nistp256] [ecdh-sha2-nistp384] [ecdh-sha2-nistp521]}

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #ip ssh server algorithm kex curve25519-sha256 ecdh-sha2-nistp384
```

no ip ssh server algorithm kex

Use this command to disable the key exchange algorithm.

Format	no ip ssh server algorithm kex {[curve25519-sha256] [curve25519-sha256@libssh.org] [diffie-hellman-group-exchange-sha256] [diffie-hellman-group14-sha1] [diffie-hellman-group14-sha256] [diffie-hellman-group16-sha512] [diffie-hellman-group18-sha512] [ecdh-sha2-nistp256] [ecdh-sha2-nistp384] [ecdh-sha2-nistp521]}

Mode	Privileged EXEC

line ssh

M4250**M4350**

This command gives you access to the SSH Config mode (Config-ssh) for a virtual terminal for secured remote console access. This mode lets you configure the secure shell (SSH) settings.

Format	line ssh
Mode	Global Config

Command example:

```
(NETGEAR Switch) (config)#line ssh
(NETGEAR Switch) (Config-ssh)#
```

show ip ssh

M4250**M4350**

This command displays the SSH settings.

Format	show ip ssh
Mode	Privileged EXEC

Term	Definition
Administrative Mode	This field indicates whether the administrative mode of SSH is enabled or disabled.
SSH Port	The SSH port in use.
Protocol Level	The protocol level shows the value of version 2.
SSH Sessions Currently Active	The number of SSH sessions currently active.
Max SSH Sessions Allowed	The maximum number of SSH sessions allowed.
SSH Timeout	The SSH time-out value in minutes.
Keys Present	Indicates if the SSH RSA, DSA, and ECDSA key files are present on the device. The length of the respective keys and the key encryption status (if the key is encrypted) are displayed in parenthesis.
Key Generation in Progress	Indicates if RSA, DSA, and ECDSA key files generation is currently in progress.

Fully Managed Switches M4250 and M4350 Series

Term	Definition
SSH Public Key Authentication Mode	Indicates if login without a password is enabled for the SSH client.
SCP Server Administrative Mode	Indicates if the SCP server is enabled on the switch. To allow file transfers from a host system to the switch using SCP push operations, the SCP server must be enabled.
Max SSH Authentication Tries	The maximum number of authentication retries supported per SSH connection.
Encryption Algorithms	The encryption algorithms used for the SSH connection.
MAC Algorithms	The Message Authentication Code algorithms used for the SSH connection.
KEX Algorithms	The Key Exchange algorithms that are used over the SSH connection.
HostKey Algorithms	The host key algorithms that are used over the SSH connection.

Command example:

```
(NETGEAR Switch)#show ip ssh
```

SSH Configuration

```
Administrative Mode: ..... Disabled
SSH Port: ..... 22
Protocol Level: ..... Version 2
SSH Sessions Currently Active: ..... 0
Max SSH Sessions Allowed: ..... 5
SSH Timeout (mins): ..... 5
Keys Present: ..... DSA(1024)
                  RSA(2048)

Key Generation In Progress: ..... None
SSH Public Key Authentication Mode: ..... Disabled
SCP server Administrative Mode: ..... Disabled
Max SSH authentication tries:..... 4
Encryption Algorithms:..... aes128-ctr
                           aes192-ctr
                           aes256-ctr

MAC Algorithms:..... hmac-sha2-256
                   hmac-sha2-512
                   hmac-sha2-256-etm@openssh.com
                   hmac-sha2-512-etm@openssh.com
```

```

KEX Algorithms:..... curve25519-sha256
                    curve25519-sha256@libssh.org
                    ecdh-sha2-nistp256
                    ecdh-sha2-nistp384
                    ecdh-sha2-nistp521
                    diffie-hellman-group-exchange-sha256
                    diffie-hellman-group16-sha512
                    diffie-hellman-group18-sha512
                    diffie-hellman-group14-sha256

HostKey Algorithms:..... rsa-sha2-256
                        rsa-sha2-512
                        ecdsa-sha2-nistp256
                        ecdsa-sha2-nistp384
                        ecdsa-sha2-nistp521

```

Management Security Commands

This section describes commands you use to generate keys and certificates, which you can do in addition to loading the keys and certificates.

crypto certificate generate

M4250

M4350

This command generates a self-signed certificate for HTTPS. This command lets the CLI enter the Crypto Certificate Generate configuration mode. The generated RSA key for SSL has a length of 2048 bits. Use the **exit** command to generate the self-signed certificate.

You can generate two certificates (1 and 2).

Format	crypto certificate {1 2} generate

Mode	Global Config

In Crypto Certificate Generate configuration mode, you can configure the following commands and arguments before using the **exit** command to generate the self-signed certificate and return to the Global Config mode.

Command	Argument	Description
common-name	<i>common-name</i>	The fully qualified URL or IP address of the device. If unspecified, this parameter defaults to the lowest IP address of the device (when the certificate is generated).
country	<i>country</i>	The country name in 2 characters

Command	Argument	Description
duration	<i>days</i>	The days range from 30 to 3650
email	<i>email</i>	The email address up to 64 characters
key-generate length	--	The length of the SSL RSA key, which is 2048 by default
location	<i>location</i>	The location or city name up to 64 characters
organization-name	<i>organization-name</i>	The organization name up to 64 characters
organization-unit	<i>organization-unit</i>	The organization unit up to 64 characters
state	<i>state</i>	The name of the state or province up to 64 characters

Command example:

```
(NETGEAR Switch) (config) #crypto certificate 1 generate
(NETGEAR Switch) (config-crypto-cert-gen) #?
common-name          Specifies the common name.
country              Specifies the country name.
do                   Run Privileged Exec mode commands.
duration              Specifies number of days a self-signed
                     certification would be valid.
email                Specifies the contact email address.
exit                 To exit from the mode.
key-generate          Regenerate SSL RSA key. If unspecified defaults to
                     1024.
location              Specifies the location or city name.
organization-name     Specifies the organization name
organization-unit     Specifies the organization internal unit
show                 Display Switch Options and Settings.
state                 Specifies the state or province name.
(NETGEAR Switch) (config-crypto-cert-gen) #
(NETGEAR Switch) (config-crypto-cert-gen) #key-generate 1024
(NETGEAR Switch) (config-crypto-cert-gen) #exit
```

Certification Generation Successful..

```
(NETGEAR Switch) (config) #
```

no crypto certificate generate

This command deletes the specified HTTPS certificate files from the switch, regardless of whether the certificate is self-signed or downloaded from an outside source.

Format	no crypto certificate {1 2}

Mode	Global Config

crypto key generate rsa

M4250

M4350

This command generates an RSA key pair with 1024, 2048 or 3072 bits for SSH. The new key files overwrite any existing generated or downloaded RSA key files.

Default	2048 bit
Format	crypto key generate rsa {1024 2048 3072}
Mode	Global Config

no crypto key generate rsa

This command deletes the RSA key files from the switch.

Format	no crypto key generate rsa
Mode	Global Config

crypto key generate dsa

M4250

M4350

This command generates a DSA key pair with 1024 bits for SSH. The new key files overwrite any existing generated or downloaded DSA key files.

Default	1024 bit
Format	crypto key generate dsa
Mode	Global Config

no crypto key generate dsa

This command deletes the DSA key files from the switch.

Format	no crypto key generate dsa
Mode	Global Config

crypto key generate ecdsa

M4250**M4350**

This command generates an ECDSA key pair with 256, 384, or 521 bits for SSH. The new key files overwrite any existing generated or downloaded ECDSA key files.

Default	None
Format	<code>crypto key generate ecdsa {256 384 521}</code>
Mode	Global Config

no crypto key generate ecdsa

This command deletes the ECDSA key files from the switch.

Format	<code>no crypto key generate ecdsa</code>
Mode	Global Config

crypto certificate request

M4250**M4350**

This command generates and displays a certificate request for HTTPS. This command lets the CLI enter the Crypto Certificate Request configuration mode. The certificate request that is generated using this command is sent to the Certification Authority for signing. The certificate request is generated in Base64-encoded X509 format. Use the **exit** command to generate the request for the self-signed certificate.

Before generating a certificate request, you must first generate a self-signed certificate using the **crypto certificate generate** command in Global Configuration mode, to sign the certificate request. Be sure to reenter the identical values in the certificate request fields as were entered in the self-signed certificate generated by the **crypto certificate generate** command. You can request two certificates.

Format	<code>crypto certificate {1 2} request</code>
Mode	Global Config

In Crypto Certificate Request configuration mode, you can configure the following commands and arguments before using the **exit** command to request the self-signed certificate and return to the Global Config mode.

Command	Argument	Description
common-name	<i>common-name</i>	The fully qualified URL or IP address of the device. If unspecified, this parameter defaults to the lowest IP address of the device (when the certificate is generated).
country	<i>country</i>	The country name in 2 characters
email	<i>email</i>	The email address up to 64 characters
location	<i>location</i>	The location or city name up to 64 characters
organization-name	<i>organization-name</i>	The organization name up to 64 characters
organization-unit	<i>organization-unit</i>	The organization unit up to 64 characters
state	<i>state</i>	The name of the state or province up to 64 characters
subject-alternative-name	<i>subjectAltName</i>	The subject alternative name in the following format: {(DNS:<name>, (IP:<Addr>))}

Command example:

```
(NETGEAR Switch) (Config)#crypto certificate 1 request
```

```
(NETGEAR Switch) (Config)#crypto certificate 1 request
```

```
(NETGEAR Switch) (config-crypto-cert-req)#?
```

```
common-name      Specifies the common name.
country          Specifies the country name.
do               Run Privileged Exec mode commands.
email            Specifies the contact email address.
exit             To exit from the mode.
location         Specifies the location or city name.
organization-name Specifies the organization name
organization-unit Specifies the organization internal unit
show             Display Switch Options and Settings.
state            Specifies the state or province name.
subject-alternative-name Specifies the Subject Alternative Name.
```

```
(Routing) (config-crypto-cert-req)# exit
```

```
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIIBUTCBuwIBA jASMRaWdGyDVQQDDAcwLjAuMCAwMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQBgQC+pfoYHFIjXe/2DDwedT1GkZKX8PP1/4F35KyaounA35kHGw9x
+y1t5hMfOererTbkLdoM8taPOYipv+gJ978DL8tNMB1MJHAcPokAmuv+PDNYaGK
sY1Y+L/Ajge7qh3iCO/HR/wPenKab4fChbyKA5x7GFriPs4YWGxbv1X2wQIDAQAB
oAAwDQYJKoZIhvcNAQELBQADgYEADXHN2ScDYGnHfTrqjl6+5XDJW66Pxi4r/JP
BVcF+QKrwItwq6AqGwJDHDVYfvc5FGnpW3vYbfovRuSalbNGmS/iUOXmpjYQryQW
```

```
AwTt2DTNPxiuZZjumfjT/utWmdFPsaibGyjcZU/HyDDFsrC7ukLWrXro6fbjvxWX
mnxt7FQ=
-----END CERTIFICATE REQUEST-----
```

Note: The Subject Alternative Name (SAN) is an extension to the X.509 specification that allows users to specify additional host names for a single SSL certificate. Some browsers do not accept the Common Name field in an SSL certificate and require the SAN field instead.

The switch supports adding the SAN field to the certificate request. The following sample SAN formats are supported.

```
DNS:example.com
```

```
DNS:*.example.com
```

```
DNS:xyz.com, IP:10.10.20.1
```

```
DNS.1:myserver.com, DNS.2:xyz.com, IP:10.10.32.1
```

crypto certificate import

M4250

M4350

This command imports a signed certificate provided by the Certification Authority (CA). The imported certificate must be based on a certificate request created by the **crypto certificate request** command. To end the session, add a period on a separate line after the input, and press **Enter**. The signed certificate must contain the switch public key, match the RSA key on the switch, and must be in X509 PEM text format. You can import two certificates.

Format	crypto certificate {1 2} import

Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config) #crypto certificate 1 import
```

Please paste the input now, add a period (.) on a separate line after the input, and press Enter.

```
-----BEGIN CERTIFICATE-----
```

```
MIIBrDCCARWgAwIBAgIJANI+zML5qmlOMA0GCSqGSIb3DQEBCwUAMBgxFjAUBgNV
BAMMDTEwLjEzMC44Ni4yMTcwHhcNNzAwMTAxMDM0MzQzWhcNNzEwMTAxMDM0MzQz
WjAYMRYwFAYDVQQDDA0xMC4xMzAuODYuMjE3MDUfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBQCZsOyuz2MlQ8ab+Y9vcRgqJdakeL8z4XLNRRDlAsNcOE6GXwskDrT8
hx0r7MywrO4J6bPfqG2t63ee3KUyPS+B6OdxwmNycRwbUZabxD87MmBwx9OtUULY
```

```
AkNCUKXG6I9kxUXry4CNbOmFtVpTHDr+xqWbmqQemRjB3VpUXOueewIDAQABMA0G
CSqGSib3DQEBECwUAA4GBAHycAeQZv80Vxcw+hWFNsWePkD6VdM8o3ecV9kcCcFuV
SreKkICC6HBuPKVxqcoVoGbBiRSMGcDJ4XD9vEWWHZv1QiIn8Z1jy+OSpEAruIOi
myM3O5cleG/4baIci1ccIJgWjwxZwAPd6kz+OtXHhWLn/+Y2akg3sev6oXLTTCsv
-----END CERTIFICATE-----
```

```
.
```

```
Certificate imported successfully
```

crypto dhparam size

M4250

M4350

This command sets the Diffie Hellman (DH) parameter. Diffie Hellman parameters are used in the Diffie-Hellman key exchange mechanism that is used while establishing SSL connections. The DH parameters are generated by the switch once and reused for all SSL connections established thereafter. While the DH parameters are being generated, the SSLT admin mode remains disabled operationally.

When the DH parameters are successfully generated, an informational message is logged to inform you that the parameters were generated and the configured DH parameter was applied.

Default	1024 bit
Format	crypto dhparam size {1024 2048}
Mode	Global Config

no crypto dhparam size

This command sets the Diffie Hellman parameter size to the default.

Format	no crypto dhparam size
Mode	Global Config

crypto key decrypt write

M4250**M4350**

This command is the equivalent of the **no crypto key encrypt** command and is used to decrypt key files with the user-provided passphrase. You select the type of key file that must be decrypted.

Format	crypto key decrypt write {rsa dsa ecdsa sslt-cert-key {1 2} sslt-client-cert-key {1-8}} passphrase <i>passphrase</i> [encrypted]

Mode	Global Config

Parameter	Definition
rsa	The RSA key pair for SSH
dsa	The DSA key pair for SSH
ecdsa	The ECDSA key pair for SSH
sslt-cert-key	The SSL certificate key (1 or 2)
slt-client-cert-key	The SSL client certificate key (from 1 to 8)
passphrase	The passphrase, which must be at least 8 characters long
encrypted	The password that is entered is encrypted

crypto key pubkey-chain ssh

M4250**M4350**

This command lets you enter the Public Key Configuration mode to manually set public keys for an individual user. After you enter the Public Key Configuration mode, you must enter the keys. When you are done, you must enter **exit**. You can set keys for either DSA or RSA.

Format	crypto key pubkey-chain ssh user-key <i>user-name</i> {dsa rsa}

Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config) #crypto key pubkey-chain ssh user-key test rsa
```

```
(NETGEAR Switch) (config-pubkey-key) #key-String "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAfvwova0rICLGoTJ46ZMRknjAk8pBEz3Y4DijzV7oim+wW7DI5mFUULI3cT11
10cjGHeQF03phufEDcK45Cr0nHCD37zDwjN5B2+YFtVq6h4dQGfBFJVnXvJ/PmqDt5iti/jAvRXn4NzHA03byn8
/yHUsrzI6Syd3FZfaBvD+Shxpgx+pZkkLRXHgZ1L/s7uxOpu6aWwjhZEFz5RjX//chT5J3uHn++W9Yt/3CwEen
ZeF4o0wEji5DTnPfkTnHxm8s4NSWHpKYOsN8LW23ooEmU0moRU0KJx7/Zeuw36fI6RvEIFbTmX6a59GRBPpaMh9
bHBAGxDA4X9x5AXTrsqS1Q=="
```

```
(NETGEAR Switch) (config-pubkey-key) #exit
```

no crypto key generate dsa

This command erases all the SSH server public key chains or the public key for a specific user.

Format	no crypto key pubkey-chain ssh user-key [user-name]
Mode	Global Config

show crypto certificate all

M4250

M4350

This command displays the root CA certificate on the switch.

Format	show crypto certificate all
Mode	Privileged Config

Command example:

```
(NETGEAR Switch)#show crypto certificate all
```

```
Root CA Certificate
```

```
Storage: nvram:ca_certs.pem
```

```
-----BEGIN CERTIFICATE-----
```

```
MIID+zCCAmOgAwIBAgIMY4CqkSlO9X3LTPA3MA0GCSqGSIb3DQEBCwUAMBKxFzAV
BgNVBAMTDkxQVAgU2VydMvYIENBMB4XDTIyMTEyNTExNDQxN1oXDTIzMTExNTEx
NDQxN1owGTEyMBUGA1UEAxMOTERBUCBTZXJ2ZXIgaQ0EwgGGM40GCSqGSIb3DQEBC
AQUAA4IBjwAwggGKAoIBgQDGejUT5V32M6wMy4XowLTmM95ft9JNW3uFXbsu0za
goFk3B/3q8LN7JbyQRZlVIEKemuLwH59SVjN2OYe29Fv9VhEbeaP3vOHIvqP8nf+
J6bVtODNH+gK3NTwwdE3kqQJpBCnMgAiIwDBXErwPmEdRN4WAdTAujoQLI3t/Qzx
GpulPNsomjJn7EXs8aIaIPN5mwvL+dwTVUwA4Urd1lnr+7orZ1vkeH5qzDp5GzeB
yYmorOAWGM3nHaP+AM//0Jx8xQJRe1Cun7GfFJchEVxMxNGqBLC9oYItNReKsKkn
yWRifQ1RibEzmrnomWVZSE5svnYF6GC/Sezg0GkZamgM4DZ/I0fMealtpSyi8S0p
LwfJF/bagFDquPbKANfW4mXq1SpXcxhPgtRoYUXqZgdmKg8TWx8EsNDJ+TNaaMxp
7R3eERBXklt6LVylAxrItTL7wFJeroq1VigKpVHnsN5AF1X29H0dhxVV56E51aaR
Th7mWh+oux87BP4jDW2ApdkCAwEAAANDMEewDwYDVR0TAQH/BAUwAwEB/zAPBgNV
HQ8BAf8EBQMDBwQAMB0GA1UdDgQWBbQbARsw6CqSAH4APL6rRYsx+JSOMjANBgkq
hkiG9w0BAQsFAAOCAYEAJlUaMqURWQp8CbEKkcYeI3jJbxAvFJrB//9YLq838xeD
vnGidioJo/cCOjBQ8ykjjAur817MO1rJesUha8u/3lFzXkCB1/zbxx9QQXTN7RKQ
6mmRIUKSWwf9nmAtol8SZ9Nb3+HaPUQLGy1b5OEruLWwUTOOGEqVh2RNRdallW+G
d42+ixizkTo/R8sOjlHSWbHqk7iaVV712iD3nSqJqu4hLgsF4Lzx/9Eel0221VS1
QPcBN1xVkBdNBXoweSBgtI4v5+TI9JFUSU5k5JrEx1iH5zExFxd7b0d9m08swsU
EKMLYjHf1vGkhEzbbLRCraytllgKfGvdA2Hw8WBWZmKlOx3OaTDCR+ic18Wm3UHL
VzTTq/3rTuY2fF1SDU9inDwseVMwtYCGFDWLiNWYoyCJ01sGU8NeYv79UJ+xZv2a
rSluB3nVmFG7P1hcX910BwkIv7460x39LXDBV7ZgkCULGw1HPKshOCEWPB7qcpaZ
9sJHksAHZbgOAcVx9ubx
```


show crypto dhparam

M4250**M4350**

This command displays the display the Diffie Hellman parameter size that is used by the SSL tunnel.

Format	show crypto dhparam

Mode	Privileged Config

Command example:

```
(NETGEAR Switch)#show crypto dhparam
DH param size ..... 1024
DH Parameter generation status ..... In progress
```

show crypto key mypubkey

M4250**M4350**

This command displays the display the SSH certificates on the switch.

Format	show crypto key mypubkey

Mode	Privileged Config

Command example:

```
(NETGEAR Switch)#show crypto key mypubkey
```

RSA Key Data:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGDl1xWi3s2eakSEsmMDoRIF748Q7pChNctFsSJOaD7esTIgGHhfFL3i2EPn
9Voh2A+8tFg2kXaiIzqWzy9kTbhmcn/tCtRyBkvmplve2z+AKwdHQx00ZzdLjtTv4/c4XTE4F6jg/LBKdhFb4+q
Gr6PekbGbuMpp4rvJF76r8wXXlsw==
Fingerprint (Hex): MD5:ad:bb:2b:dd:c0:4b:8e:bc:f1:99:35:05:25:00:d5:cd
Fingerprint (Bubble Babble):
xicag-duvek-fulir-lelab-sumyk-selar-suzys-fopum-cavis-gebyh-coxax
```

DSA Key Data:

```
ssh-dss
AAAAB3NzaC1kc3MAAACBANrQifFkVewhGrGtOM8tzm1gig7vdp3zRY81jIiQF8ukS8x2f/WDPaUlaZa+wf8pmt0
y+nAv9rPmYTdnM0Ife8X+uu669xd15+FWkrSqe8B6c1NXVDJxDqJlGqOuNjxBj5W+hzvWQODTndVJm9L23hi+0z
xt0DcWfvFVJILFNhJHAAAFQC00qsPDniPrEn7wNUZH2r2mwGohwAAAIBECr5kreyIwwVBXq05yuSc+khzQ5aDd
HBaEKk4RIqqGjCZTEZOZxzsQD+OSndE5lo6GBKQdA577Nfoo3SzmffwAAAI EA04qsYl2WD1NBf86Ga7kX1EZYpVy
No8tmz3tk899P4VoZFRDw9BzrC/j723Vd127j0u8oddJKwliXWFSi4nbWg5NdiaSxtBH5v0nzs3GK59QIirXAJp
3ZKMaTzn26PTlemLpw9zxwDpjRLmtpUIKG464KZQwIzSjhcWDJAgDmyVU=
```

```
Fingerprint (Hex): MD5:50:4e:c7:aa:ff:41:48:0f:f1:f6:46:4a:1e:db:e2:a7
Fingerprint (Bubble Babble):
xomal-radyc-rebid-hodid-gelos-pekyn-voduz-cidom-damen-mogeb-hoxox
```

show crypto key pubkey-chain ssh

M4250

M4350

This command displays the SSH client's public keys on the switch.

Use the optional **fingerprint** keyword with either the **bubble-babble** or **hex** keyword to display the keys per finger print in the bubble babble format or the hexadecimal format.

Use the optional **username** keyword and associated *name* argument to display the keys per user name. The **fingerprint** keyword with either the **bubble-babble** or **hex** keyword are optional.

Format	show crypto key pubkey-chain ssh [fingerprint {bubble-babble hex} username <i>name</i> [fingerprint {bubble-babble hex}]]
Mode	Privileged Config

Command example:

```
(NETGEAR Switch)#show crypto key pubkey-chain ssh
```

```
Username                               Fingerprint
-----
test      MD5:19:8c:81:e3:cd:5c:2a:8a:91:cb:5e:35:a4:43:93:91
```

Management Access Control List Commands

You can use a management access control list (ACL) to help control access to the switch management interface. A management ACL can help ensure that only known and trusted devices are allowed to remotely manage the switch via TCP/IP.

After you define a management ACL name, you enter the management access control and administration list CLI mode (config-macal CLI mode), which lets you configure the ACL. We refer to this mode as the Management access-list configuration mode.

When you enable a management ACL, incoming TCP packets initiating a connection (TCP SYN) and all UDP packets are filtered. When you disable the management ACL, incoming TCP/UDP packets are not filtered and are processed normally.

management access-list

M4250**M4350**

This command creates a management ACL. The management ACL name can be up to 32 alphanumeric characters. Executing this command enters into access-list configuration mode, from which you must define the denied or permitted access conditions with the **deny** and **permit** commands. If no match criteria are defined the default is to deny access (*deny*). If you reenter to an access-list context, new rules are entered at the end of the access list.

Format	management access list <i>name</i>
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config) #management access-list ACLNAME
(NETGEAR Switch) (config-macal) #
```

no management access-list

This command deletes a management ACL identified by the *name* parameter.

Format	no management access list <i>name</i>
Mode	Global Config

deny | permit (Management access-list configuration)

M4250**M4350**

This command sets a deny or permit condition for the management access list based on the Ethernet interface, VLAN ID, port channel number, service port, service type, priority, or a combination of all of these for the rule. Each rule requires a unique priority. Use this command in Management access-list configuration mode.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	{deny permit} [ethernet <i>unit/slot/port</i> vlan <i>vlan-id</i> port-channel <i>lag-group-id</i> serviceport] [service <i>service</i>] [priority <i>priority</i>]
Mode	Management access-list configuration

Parameter	Definition
ethernet <i>unit/slot/port</i>	The number of the Ethernet interface.
vlan <i>vlan-id</i>	The VLAN ID.
port-channel <i>lag-group-id</i>	The number of the port-channel.
service <i>service</i>	The service type for the rule, which can be one of the following keywords: • 1 to 65535: A TCP or /UDP port number, which you must specify. • tftp • telnet • ssh • http • https • snmp • ntp • any
priority <i>priority</i>	The priority for the rule, which is a number in the range from 1 to 64.

Command example:

The following example shows how to configure two management interfaces, ethernet 1/0/2 and ethernet 1/0/9:

```
(NETGEAR Switch) (Config)#management access-list mlist
(NETGEAR Switch) (config-macal)#permit ethernet 1/0/2 priority 63
(NETGEAR Switch) (config-macal)#permit ethernet 1/0/9 priority 64
(NETGEAR Switch) (config-macal)#exit
(NETGEAR Switch) (Config)#
```

Command example:

The following example shows how to configure all the interfaces to be management interfaces except for interfaces ethernet 1/0/2 and ethernet 1/0/9:

```
(NETGEAR Switch) (Config)#management access-list mlist
(NETGEAR Switch) (config-macal)#deny ethernet 0/1 priority 62
(NETGEAR Switch) (config-macal)#deny ethernet 0/9 priority 63
(NETGEAR Switch) (config-macal)#permit priority 64
(NETGEAR Switch) (config-macal)#exit
(NETGEAR Switch) (Config)#
```

deny | permit ip-source (Management access-list configuration)

M4250**M4350**

This command sets a deny or permit condition for the management access list based on the source IP address of a packet. Optionally, you can specify a subnet mask prefix length, Ethernet interface, VLAN ID, port channel number, service port, service type, priority, or a combination of all of these for the rule. Each rule requires a unique priority. Use this command in Management access-list configuration mode.

Format	{deny permit} ip-source <i>ip-address</i> [mask <i>mask</i> <i>prefix-length</i>] [ethernet <i>unit/slot/port</i> vlan <i>vlan-id</i> port-channel <i>lag-group-id</i> serviceport] [service <i>service</i>] [priority <i>priority</i>]
Mode	Management access-list configuration
Parameter	Definition
<i>ip-address</i>	The source IPv4 or IPV6 address.
mask <i>mask</i>	The network mask of the source IP address.
<i>prefix-length</i>	The number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/).
ethernet <i>unit/slot/port</i>	The number of the Ethernet interface.
vlan <i>vlan-id</i>	The VLAN ID.
port-channel <i>lag-group-id</i>	The number of the port-channel.
service <i>service</i>	The service type for the rule, which can be one of the following keywords: • 1 to 65535: A TCP or /UDP port number, which you must specify. • tftp • telnet • ssh • http • https • snmp • ntp • any
priority <i>priority</i>	The priority for the rule, which is a number in the range from 1 to 64.

management access-class

M4250**M4350**

This command activates the configured management ALC and restricts management connections within the management ACL. The *name* parameter is the name of the existing management ACL. You cannot update or remove a management ACL when it is active.

Format	management access-class <i>name</i>

Mode	Global Config

no management access-class

This command disables a management ACL.

Format	no management access-class

Mode	Global Config

show management access-list

M4250**M4350**

This command displays information about the configured management ALC.

Format	show management access-list [<i>name</i>]

Mode	Privileged EXEC

Field	Definition
List Name	The name of the management ACL
List Admin Mode	The administrative mode of the management ACL. To activate a management ACL, enter the management access-class command (see management access-class on page 109).
Packets Filtered	The number of packets filtered by the management ACL
Rules	The rules that are included in the ACL.

Command example:

```
(NETGEAR Switch) #show management access-list
```

```
List Name..... mgmtacl
List Admin Mode..... Disabled
Packets Filtered..... 0
```

```
Rules:
```

```

permit ip-source 192.168.2.10 mask 255.255.255.255 service ssh priority 1
permit ip-source 192.168.2.182 mask 255.255.255.255 service ssh priority 2
permit ip-source 192.168.2.23 mask 255.255.255.255 service ssh priority 3

```

NOTE: All other access is implicitly denied.

show management access-class

M4250

M4350

This command displays information about the configured management ACL.

Format	show management access-class
Mode	Privileged EXEC
Field	Definition
List Name	The name of the management ACL
List Admin Mode	The administrative mode of the management ACL. To activate a management ACL, enter the management access-class command (see management access-class on page 109).
Packets Filtered	The number of packets filtered by the management ACL

Command example:

```
(NETGEAR Switch) #show management access-class
```

```

List Name..... mgmtacl
List Admin Mode..... Disabled
Packets Filtered..... 0

```

Hypertext Transfer Protocol Commands

M4250

M4350

This section describes the commands you use to configure Hypertext Transfer Protocol (HTTP) and secure HTTP access to the switch. Access to the switch by using a Web browser is enabled by default. Everything you can view and configure by using the CLI is also available by using the web.

ip http accounting exec

This command applies user exec (start-stop/stop-only) accounting list to the line method HTTP.

Note: The user exec accounting list must be created using the command [aaa accounting on page 154](#).

Format	<code>ip http accounting exec {default listname}</code>

Mode	Global Config

Parameter	Description
http	The line method for which the list needs to be applied.
default	The default list of methods for authorization services.
listname	An alphanumeric character string used to name the list of accounting methods.

no ip http accounting exec

This command deletes the authorization method list.

Format	<code>no ip http accounting exec {default listname}</code>

Mode	Global Config

ip https accounting exec

M4250

M4350

This command applies user exec (start-stop/stop-only) accounting list to the line method HTTPS.

Note: The user exec accounting list must be created using the command [aaa accounting on page 154](#).

Format	<code>ip https accounting exec {default listname}</code>

Mode	Global Config

Parameter	Description
https	The line method for which the list needs to be applied.
default	The default list of methods for authorization services.
listname	An alphanumeric character string used to name the list of accounting methods.

no ip https accounting exec

This command deletes the authorization method list.

Format	no ip https accounting exec {default listname}
Mode	Global Config

ip http authentication

M4250

M4350

Use this command to specify authentication methods for http server users. The default configuration is the local user database is checked. This action has the same effect as the command **ip http authentication local**. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

For example, if **none** is specified as an authentication method after **radius**, no authentication is used if the RADIUS server is down.

Default	local
Format	ip http authentication method1 [method2...]
Mode	Global Config

Parameter	Description
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Command example:

The following example configures http authentication:

```
(NETGEAR Switch) (config)# ip http authentication radius local
```

no ip http authentication

Use this command to return to the default.

Format	no ip http authentication

Mode	Global Config

ip https authentication

M4250

M4350

Use this command to specify authentication methods for https server users. The default configuration is the local user database is checked. This action has the same effect as the command **ip https authentication local**. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line. For example, if **none** is specified as an authentication method after **radius**, no authentication is used if the RADIUS server is down.

Default	local

Format	ip https authentication method1 [method2...]

Mode	Global Config

Parameter	Description

local	Uses the local username database for authentication.

none	Uses no authentication.

radius	Uses the list of all RADIUS servers for authentication.

tacacs	Uses the list of all TACACS+ servers for authentication.

Command example:

The following example configures http authentication:

```
(NETGEAR Switch) (config) # ip https authentication radius local
```

no ip https authentication

Use this command to return to the default.

Format	no ip https authentication

Mode	Global Config

ip http server

M4250

M4350

This command enables access to the switch through the Web interface. When access is enabled, the user can login to the switch from the Web interface. When access is disabled, the user cannot login to the switch's Web server. Disabling the Web interface takes effect immediately. All interfaces are affected.

Default	enabled
Format	ip http server
Mode	Privileged EXEC

no ip http server

This command disables access to the switch through the Web interface. When access is disabled, the user cannot login to the switch's Web server.

Format	no ip http server
Mode	Privileged EXEC

ip http secure-server

M4250

M4350

This command is used to enable the secure socket layer for secure HTTP.

Default	disabled
Format	ip http secure-server
Mode	Privileged EXEC

no ip http secure-server

This command is used to disable the secure socket layer for secure HTTP.

Format	no ip http secure-server
Mode	Privileged EXEC

ip http port

M4250

M4350

Use this command to configure the TCP port number on which the HTTP server detects requests. The *number* argument can be a port number in the range from 1 to 65535.

Default	80
Format	ip http port <i>number</i>
Mode	Privileged EXEC

no ip http port

Use this command to reset the TCP port number on which the HTTP server detects requests to the default of 80.

Format	no ip http port
Mode	Privileged EXEC

ip http session hard-timeout

M4250

M4350

This command configures the hard time-out for unsecure HTTP sessions. The time-out value unit of time is hours and is specified by the *hours* argument in the range 1–168 hours. Configuring this value to zero will give an infinite hard-time-out. When this time-out expires, the user will be forced to reauthenticate. This timer begins on initiation of the web session and is unaffected by the activity level of the connection.

Default	24
Format	ip http session hard-timeout <i>hours</i>
Mode	Privileged EXEC

no ip http session hard-timeout

This command restores the hard time-out for un-secure HTTP sessions to the default value.

Format	no ip http session hard-timeout
Mode	Privileged EXEC

ip http session maxsessions

M4250

M4350

This command limits the number of allowable unsecure HTTP sessions. The *number* argument specifies the number of sessions in the range of 0–16. Zero is the configurable minimum.

Default	16
Format	ip http session maxsessions <i>number</i>
Mode	Privileged EXEC

no ip http session maxsessions

This command restores the number of allowable un-secure HTTP sessions to the default value.

Format	no ip http session maxsessions
Mode	Privileged EXEC

ip http session soft-timeout

M4250

M4350

This command configures the soft time-out for un-secure HTTP sessions. The time-out value unit of time is minutes and is specified by the *minutes* argument in the range 1–60 minutes. Configuring this value to zero will give an infinite soft-time-out. When this time-out expires the user will be forced to reauthenticate. This timer begins on initiation of the Web session and is restarted with each access to the switch.

Default	5
Format	ip http session soft-timeout <i>minutes</i>
Mode	Privileged EXEC

no ip http session soft-timeout

This command resets the soft time-out for un-secure HTTP sessions to the default value.

Format	no ip http session soft-timeout
Mode	Privileged EXEC

ip http secure-session hard-timeout

M4250

M4350

This command configures the hard time-out for secure HTTP sessions. The time-out value unit of time is hours and is specified by the *hours* argument in the range 1–168 hours. When this time-out expires, the user is forced to reauthenticate. This timer begins on initiation of the Web session and is unaffected by the activity level of the connection. The secure-session hard-time-out can not be set to zero (infinite).

Default	24
Format	ip http secure-session hard-timeout <i>hours</i>
Mode	Privileged EXEC

no ip http secure-session hard-timeout

This command resets the hard time-out for secure HTTP sessions to the default value.

Format	no ip http secure-session hard-timeout
Mode	Privileged EXEC

ip http secure-session maxsessions

M4250

M4350

This command limits the number of secure HTTP sessions. The *number* argument specifies the number of sessions in the range of 0–16. Zero is the configurable minimum.

Default	16
Format	ip http secure-session maxsessions <i>number</i>
Mode	Privileged EXEC

no ip http secure-session maxsessions

This command restores the number of allowable secure HTTP sessions to the default value.

Format	no ip http secure-session maxsessions
Mode	Privileged EXEC

ip http secure-session soft-timeout

M4250

M4350

This command configures the soft time-out for secure HTTP sessions. The time-out value unit of time is minutes and is specified by the *minutes* argument in the range 1–60 minutes. Configuring this value to zero will give an infinite soft-time-out. When this time-out expires, you are forced to reauthenticate. This timer begins on initiation of the Web session and is restarted with each access to the switch. The secure-session soft-time-out can not be set to zero (infinite).

Default	5
Format	ip http secure-session soft-timeout <i>minutes</i>
Mode	Privileged EXEC

no ip http secure-session soft-timeout

This command restores the soft time-out for secure HTTP sessions to the default value.

Format	no ip http secure-session soft-timeout
Mode	Privileged EXEC

ip http secure-port

M4250

M4350

Use this command to set the SSL port number. The port number can be from 1025 to 65535, and the default is port number 443.

Default	443
Format	ip http secure-port <i>portid</i>
Mode	Privileged EXEC

no ip http secure-port

Use this command to reset the SSL port to the default value (443).

Format	no ip http secure-port
Mode	Privileged EXEC

ip http secure-certificate

M4250**M4350**

Use this command to configure the active certificate for HTTPS. The switch supports two certificates.

Format	<code>ip http secure-certificate {1 2}</code>
Mode	Privileged EXEC

ip http secure-ciphersuite

M4250**M4350**

Use this command to specify the cipher suites to be used over an HTTPS connection. If you do not specify the cipher suites, the server and the client negotiate a connection with the cipher suite that they both can support.

Default	All cipher suite options are enabled by default.
Format	<code>ip http secure-ciphersuite {[aes-128-cbc-sha][aes-256-cbc-sha] [dhe-aes-128-cbc-sha][dhe-aes-cbc-sha2][dhe-aes-gcm-sha2] [ecdhe-rsa-aes-cbc-sha2][ecdhe-rsa-aes-gcm-sha2][ecdhe-rsa-chacha-poly-sha2] [rsa-aes-cbc-sha2][rsa-aes-gcm-sha2]}</code>
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #ip http secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha
dhe-aes-128-cbc-sha dhe-aes-cbc-sha2
```

show ip http

This command displays the http settings for the switch.

Format	<code>show ip http</code>
Mode	Privileged EXEC

Term	Definition
HTTP Mode (Unsecure)	The insecure HTTP server administrative mode.
HTTP Port	The insecure HTTP server port number
Maximum Allowable HTTP Sessions	The number of allowable un-secure http sessions.

Term	Definition
HTTP Session Hard Timeout	The hard time-out for insecure http sessions in hours.
HTTP Session Soft Timeout	The soft time-out for insecure http sessions in minutes.
HTTP Mode (Secure)	The secure HTTP server administrative mode.
HTTP Operational Mode	The secure HTTP server operational mode.
Secure Port	The secure HTTP server port number.
Secure Protocol Level(s)	The protocol level can be SSL3 or TLS 1.2.
Maximum Allowable HTTPS Sessions	The number of allowable secure http sessions.
HTTPS Session Hard Timeout	The hard time-out for secure http sessions in hours.
HTTPS Session Soft Timeout	The soft time-out for secure http sessions in minutes.
Certificate Present	Indicates if the secure-server certificate files are present on the switch.
User Selected Certificate	The number of user-selected certificates, if any.
Active Certificate	The number of active certificates, if any.
Expired Certificate	The number of expired certificates, if any.
Certificate Generation in Progress	Indicates if certificate generation is in progress.
DH Key Exchange	Indicates if DH key exchange is enabled.

Access Commands

Use the commands in this section to close remote connections or to view information about connections to the system.

disconnect

M4250

M4350

Use the `disconnect` command to close HTTP, HTTPS, Telnet or SSH sessions. Use `all` to close all active sessions, or use `session-id` to specify the session ID to close. To view the possible values for `session-id`, use the `show login session` command.

Format `disconnect {session-id | all}`

Mode Privileged EXEC

show login session

M4250

M4350

This command displays current Telnet, SSH and serial port connections to the switch. This command displays truncated user names. Use the **show login session long** command to display the complete usernames.

Format	show login session
Mode	Privileged EXEC
Term	Definition
ID	Login Session ID.
User Name	The name the user entered to log on to the system.
Connection From	IP address of the remote client machine or EIA-232 for the serial port connection.
Idle Time	Time this session has been idle.
Session Time	Total time this session has been connected.
Session Type	Shows the type of session, which can be HTTP, HTTPS, telnet, serial, or SSH.

show login session long

M4250

M4350

This command displays the complete user names of the users currently logged in to the switch.

Format	show login session long
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show login session long
User Name
-----
admin
test1111test1111test1111test1111test1111test1111test1111test1111
```

User Account Commands

This section describes the commands you use to add, manage, and delete switch users. The switch provides two default users: admin and guest. The admin user can view and configure the switch settings. The guest user can view the switch settings only.

The first time that you log in as an admin user, no password is required (that is, the password is blank). After you log in for the first time, you are required to specify a new password that you must use each subsequent time that you log in. After you specify the new password, you are logged out and then must log in again, using your new password.

The default guest user cannot log in until the admin user specifies a password for the guest user.

You cannot reset the new password to the default password. For example, if you enter the **username admin nopassword** command, the password is not reset to the default password.

However, if you enter the **clear-config** command, the passwords for the default admin user and default guest user are reset to defaults. In such a situation, the admin user must again specify a new password after logging in for the first time. Similarly, the admin user must again specify a password for the default guest user.

Note: You cannot delete the admin user, which is the only user with read/write privileges on the switch. You can configure up to five read-only users (that is, guest users) on the switch.

aaa authentication login

M4250

M4350

Note: A user with privilege level 1 cannot enter in Privilege Exec Mode and cannot execute Privilege Exec commands.

Use this command to set authentication at login. The default and optional list names created with the command are used with the **aaa authentication login** command. Create a list by entering the **aaa authentication login list-name method** command, where **list-name** is any character string used to name this list. The **method** argument identifies the list of methods that the authentication algorithm tries, in the specified sequence.

The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

For example, if **none** is specified as an authentication method after **radius**, no authentication is used if the RADIUS server is down.

If you configure **local** as the first method in the list, the switch tries no other methods.

Default	• defaultList. Used by the console and only contains the method none. • networkList. Used by telnet and SSH and only contains the method local.
Format	<code>aaa authentication login {default list-name} method1 [method2...]</code>
Mode	Global Config
Parameter	Definition
default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
list-name	Character string of up to 15 characters used to name the list of authentication methods activated when a user logs in.
method1... [method2...]	At least one from the following: • enable. Uses the enable password for authentication. • line. Uses the line password for authentication. • local. Uses the local username database for authentication. • none. Uses no authentication. • radius. Uses the list of all RADIUS servers for authentication. • tacacs. Uses the list of all TACACS servers for authentication.

Command example:

```
(NETGEAR Switch)(config)# aaa authentication login default radius local enable none
```

no aaa authentication login

This command returns to the default.

Format	<code>aaa authentication login {default list-name}</code>
Mode	Global Config

aaa authentication enable

M4250

M4350

Use this command to set authentication for accessing higher privilege levels. The default enable list is **enableList**. It is used by console, and contains the method as **enable** followed by **none**.

A separate default enable list, **enableNetList**, is used for Telnet and SSH users instead of **enableList**. This list is applied by default for Telnet and SSH, and contains **enable** followed by **deny** methods. By default, the enable password is not configured. That means

that, by default, Telnet and SSH users will not get access to Privileged EXEC mode. On the other hand, with default conditions, a console user always enter the Privileged EXEC mode without entering the **enable** password.

The default and optional list names created with the **aaa authentication enable** command are used with the **enable authentication** command. Create a list by entering the **aaa authentication enable list-name method** command where **list-name** is any character string used to name this list. The **method** argument identifies the list of methods that the authentication algorithm tries in the specified sequence.

The user manager returns ERROR (not PASS or FAIL) for enable and line methods if no password is configured, and moves to the next configured method in the authentication list. The method **none** reflects that there is no authentication needed.

The user will only be prompted for an enable password if one is required. The following authentication methods do not require passwords:

- none
- deny
- enable (if no enable password is configured)
- line (if no line password is configured)

See the examples below.

1. **aaa authentication enable default enable none**
2. **aaa authentication enable default line none**
3. **aaa authentication enable default enable radius none**
4. **aaa authentication enable default line tacacs none**

Examples 1 and 2 do not prompt for a password, however because examples 3 and 4 contain the radius and tacacs methods, the password prompt is displayed.

If the login methods include only enable, and there is no enable password configured, the switch does not prompt for a user name. In such cases, the switch prompts only for a password. The switch supports configuring methods after the local method in authentication and authorization lists. If the user is not present in the local database, then the next configured method is tried.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

Use the command [show authorization methods on page 132](#) to display information about the authentication methods.

Note: Requests sent by the switch to a RADIUS or TACACS server include the username `$enabx$`, in which **x** is the requested privilege level. The login user ID is also sent to a TACACS+ server.

Default	default
Format	aaa authentication enable {default <i>list-name</i> } <i>method1</i> [<i>method2...</i>]
Mode	Global Config

Parameter	Description
default	Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.
list-name	Character string used to name the list of authentication methods activated, when using access higher privilege levels. Range: 1-15 characters.
method1 [method2...]	Specify at least one from the following: - deny. Used to deny access. - enable. Uses the enable password for authentication. - line. Uses the line password for authentication. - none. Uses no authentication. - radius. Uses the list of all RADIUS servers for authentication. - tacacs. Uses the list of all TACACS+ servers for authentication.

Command example:

The following example sets authentication to access higher privilege levels:

```
(NETGEAR Switch) (config)# aaa authentication enable default enable
```

no aaa authentication enable

Use this command to return to the default configuration.

Format	no aaa authentication enable {default <i>list-name</i> }
Mode	Global Config

aaa authorization

M4250

M4350

Use this command to configure command and exec authorization method lists. This list is identified by **default** or a user-specified *list-name*. If **tacacs** is specified as the authorization method, authorization commands are notified to a TACACS+ server. If **none** is

specified as the authorization method, command authorization is not applicable. A maximum of five authorization method lists can be created for the **commands** type.

Note: The local method is not supported for command authorization. Command authorization with RADIUS functions only if the applied authentication method is also RADIUS.

Format	<code>aaa authorization {exec commands} {default <i>list-name</i>} <i>method1</i> [<i>method2</i>...]</code>
Mode	Global Config
Term	Definition
exec	Provides authorization for user EXEC terminal sessions.
commands	Provides authorization for all user-executed commands.
default	The default list of methods for authorization services.
list-name	Character string used to name the list of authorization methods.
method1 [method2...]	Use either tacacs or radius for authorization purpose.

no aaa authorization

This command deletes the authorization method list.

Format	<code>no aaa authorization {exec commands} {default <<i>list-name</i>>} <<i>method1</i>> [<<i>method2</i>>...]</code>
Mode	Global Config

mfa-enable

M4250

M4350

This command enables the multi-factor authentication (MFA) feature at the global level.

Default	enabled
Format	<code>mfa-enable</code>
Mode	Global Config

no mfa-enable

This command disables the MFA feature at the global level.

Format	no mfa-enable

Mode	Global Config

show mfa

M4250

M4350

This command displays if multi-factor authentication (MFA) is globally enabled for all users for whom authentication is performed based on the switch user accounts configuration.

Format	show mfa

Mode	Privileged Config

show mfa log

M4250

M4350

This command displays buffered multi-factor authentication login logs. The switch records the most recent MFA login logs.

Format	show mfa log

Mode	Privileged Config

Command example:

```
#show mfa log
```

Multifactor Authentication logs:

```
1970-01-01T00:02:12.644+0:00Z dhcp-10-52-143-61 : Requested to enter OTP for session
id-2:
1970-01-01T00:02:12.645+0:00Z dhcp-10-52-143-61 : Unable to send multifactor
authentication code to the configured
email for login user 'test'.
1970-01-01T00:03:01.059+0:00Z dhcp-10-52-143-61 : Requested to enter OTP for session
id-2:
1970-01-01T00:08:01.063+0:00Z dhcp-10-52-143-61 : Multifactor authentication OTP has
expired for session id: 2.
1970-01-01T00:08:16.674+0:00Z dhcp-10-52-143-61 : Requested to enter OTP for session
id-2:
1970-01-01T00:08:26.933+0:00Z dhcp-10-52-143-61 : Incorrect OTP entered. Retrying again
for session id: 2.
```

```
1970-01-01T00:08:42.128+0:00Z dhcp-10-52-143-61 : MFA OTP authentication is success for
session id: 2.
```

Per-Command Authorization

When authorization is configured for a line mode, the user manager sends information about an entered command to the AAA server. The AAA server validates the received command, and responds with either a PASS or FAIL response. If approved, the command is executed. Otherwise, the command is denied and an error message is shown to the user. The various utility commands such as tftp, ping, and outbound telnet should also pass command authorization. Applying the script is treated as a single command apply script, which also goes through authorization. Startup-config commands applied on device boot-up are not an object of the authorization process.

The per-command authorization usage scenario is this:

1. Configure Authorization Method List

```
aaa authorization commands listname tacacs radius none
```
2. Apply AML to an Access Line Mode (console, telnet, SSH)

```
authorization commands listname
```
3. Commands entered by the user will go through command authorization via TACACS+ or RADIUS server and will be accepted or denied.

Exec Authorization

When exec authorization is configured for a line mode, the user may not be required to use the enable command to enter Privileged EXEC mode. If the authorization response indicates that the user has sufficient privilege levels for Privileged EXEC mode, then the user bypasses User EXEC mode entirely.

The exec authorization usage scenario is as follows:

1. Configure Authorization Method List

```
aaa authorization exec listname method1 [method2....]
```
2. Apply AML to an Access Line Mode (console, telnet, SSH)

```
authorization exec listname
```
3. When the user logs in, in addition to authentication, authorization will be performed to determine if the user is allowed direct access to Privileged EXEC mode.

Format	<code>aaa authorization {commands exec} {default list-name} method1 [method2]</code>
Mode	Global Config

Parameter	Description
commands	Provides authorization for all user-executed commands.
exec	Provides exec authorization.
default	The default list of methods for authorization services.
list-name	Alphanumeric character string used to name the list of authorization methods.
method	TACACS+, RADIUS, Local, and none are supported.

```
(NETGEAR Switch) #
(NETGEAR Switch) #configure
(NETGEAR Switch) (Config)#aaa authorization exec default tacacs+ none
(NETGEAR Switch) (Config)#aaa authorization commands default tacacs+ none
```

no aaa authorization

This command deletes the authorization method list.

Format	no aaa authorization {commands exec} {default list-name}
Mode	Global Config

authorization commands

M4250

M4350

This command applies a command authorization method list to an access method (console, Telnet, SSH). After you enter this command, command authorization is required for each command execution attempt.

- Access the Line Config mode by entering the **line console** command from the Global Config mode.
- Access the SSH Config mode by entering the **line ssh** command from the Global Config mode.
- Access the Telnet Config mode by entering the **line telnet** command from the Global Config mode.

For usage scenarios on per command authorization, see the command [aaa authorization on page 125](#).

Format	authorization commands [default list-name]
Mode	Line Config SSH Config Telnet Config

no authorization commands

This command removes command authorization from a configuration in Line Config, SSH Config, or Telnet Config mode.

Format	no authorization {commands exec}

Mode	Line Config Telnet Config SSH Config

Command example:

```
(NETGEAR Switch) (Config)#line console
(NETGEAR Switch) (Config-line)#authorization commands list2

(NETGEAR Switch) (Config-line)#
(NETGEAR Switch) (Config-line)#exit
```

authorization exec

M4250

M4350

This command applies a command authorization method list to an access method so that the user may not be required to use the enable command to enter Privileged EXEC mode.

- Access the Line Config mode by entering the **line console** command from the Global Config mode.
- Access the SSH Config mode by entering the **line ssh** command from the Global Config mode.
- Access the Telnet Config mode by entering the **line telnet** command from the Global Config mode.

For usage scenarios on exec authorization, see the command [aaa authorization on page 125](#).

Format	authorization exec <i>list-name</i>

Mode	Line Config SSH Config Telnet Config

Parameter	Description
list-name	The command authorization method list.

no authorization exec

This command removes command authorization from a configuration in Line Config, SSH Config, or Telnet Config mode.

Format	no authorization exec
Mode	Line Config SSH Config Telnet Config

authorization exec default

M4250

M4350

This command applies a default command authorization method list to an access method so that the user may not be required to use the enable command to enter Privileged EXEC mode.

- Access the Line Config mode by entering the **line console** command from the Global Config mode.
- Access the SSH Config mode by entering the **line ssh** command from the Global Config mode.
- Access the Telnet Config mode by entering the **line telnet** command from the Global Config mode.

For usage scenarios on exec authorization, see the command [aaa authorization on page 125](#).

Format	authorization exec default
Mode	Line Config SSH Config Telnet Config

no authorization exec default

This command removes command authorization from the Line Config, SSH Config, or Telnet Config mode.

Format	no authorization exec default
Mode	Line Config SSH Config Telnet Config

show authorization methods

M4250**M4350**

This command displays the configured authorization method lists.

Format	show authorization methods

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show authorization methods
```

```
Command Authorization List      Method
-----
dfltCmdAuthList                tacacs      none
list2                          none        undefined
list4                          tacacs      undefined
```

```
Line      Command Method List
-----
Console   dfltCmdAuthList
Telnet    dfltCmdAuthList
SSH       dfltCmdAuthList
```

```
Exec Authorization List      Method
-----
dfltExecAuthList             tacacs      none
list2                        none        undefined
list4                        tacacs      undefined
```

```
Line      Exec Method List
-----
Console   dfltExecAuthList
Telnet    dfltExecAuthList
SSH       dfltExecAuthList
```


enable authentication (Line Config)

M4250

M4350

Use this command to specify the authentication method list when accessing a higher privilege level from a remote telnet or console.

Format	<code>enable authentication {default list-name}</code>
Mode	Line Config
Parameter	Description
default	Uses the default list created with the <code>aaa authentication enable</code> command.
list-name	Uses the indicated list created with the <code>aaa authentication enable</code> command.

Command example:

The following example specifies the default authentication method to access a higher privilege level console:

```
(NETGEAR Switch) (config) # line console
(NETGEAR Switch) (config-line) # enable authentication default
```

no enable authentication (Line Config)

Use this command to return to the default specified by the `enable authentication` command.

Format	<code>no enable authentication</code>
Mode	Line Config

username (Global Config)

M4250

M4350

This command adds a new user to the local user database, allowing the user to enter a password in plain text. However, the password is displayed as a series of asterisks (*). That is, when you configure a user password, the password does not display in clear text but encrypted. The exception is when you enter the command in the following format that includes the `encrypted` keyword:

- `username name password password level level encrypted [override-complexity-check]`
- `username name password password {encryption-type {sha256 | sha512}} encrypted [override-complexity-check]`

- **username** *name* **password** *password* {**encryption-type** {**sha256** | **sha512**}} **level** *level* **encrypted** [**override-complexity-check**]

In these situations, the entered password (as in *password*) does display in clear text.

For a new user, the default (privilege) level is 1.

The optional parameter **override-complexity-check** disables the validation of the password strength.

You can also use the **email-id** keyword and associated *email-address* argument to set an email address for the user, and as an option, use the **mfa-enable** keyword to enable multi-factor authentication for the user.

Format `username name {password password [encryption-type {sha256 | sha512}}
[encrypted [override-complexity-check] | level level [encrypted
[override-complexity-check]] | override-complexity-check}} | {level level
[override-complexity-check] password password [encryption-type
encryption-type}} [email-id email-address] [mfa-enable]}`

Mode Global Config

Parameter	Description
<i>name</i>	The name of the user. The range is from 1 to 64 characters.
password <i>password</i>	Indicates that the user must enter a plain text password. This password must range from 8 to 64 characters. Even though the password is entered in plain text, the password is shown as a series of asterisks (*). The special characters allowed in the password include the following: ! # \$ % & ' () * + , - . / : ; < = > @ [\] ^ _ ` { } ~. The password length can be zero if the no passwords min-length command is executed.
encryption-type <i>sha256</i> <i>sha512</i>	The encryption algorithm type, which can be SHA-512 (the default) or SHA-256.
override-complexity-check	Disables the validation of the password strength.
level <i>level</i>	The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. The range is from 0 to 15. Enter access level 1 for Read Access or 15 for Read/Write Access. In a situation in which the level is optional and you do not specify it, the level is set to 1.
encrypted	Requires an encrypted password to be entered or copied from another switch configuration.
email-id <i>email-address</i>	The email address for the user.
mfa-enable	Enables the multi-factor authentication feature at the user level.

Command example:

The following example configures a password for the user “bob” with (privilege) level 15:

```
(NETGEAR Switch) (Config) #username bob level 15 password
```

```
Enter new password:*****
```

```
Confirm new password:*****
```

Command example:

The following example configures a password for the user “test123” with (privilege) level 15, and the encryption set to SHA-512:

```
(NETGEAR Switch) (Config) #username test123 level 15 password encryption-type sha512
```

```
Enter new password:*****
```

```
Confirm new password:*****
```

Command example:

The following example configures a password for the user “test1234” with the **override-complexity-check password** keyword set:

```
(NETGEAR Switch) (Config) #username test1234 override-complexity-check password
```

```
Enter new password:*****
```

```
Confirm new password:*****
```

no username

Use this command to remove a user name.

Format	no username <i>name</i>

Mode	Global Config

username name nopassword

M4250

M4350

This command removes an existing user’s password (NULL password).

Format	username <i>name</i> nopassword [<i>level level</i>]

Mode	Global Config

Parameter	Description
name	The name of the user. Range: 1-32 characters.
password	The authentication password for the user. Range 8-64 characters.
level	The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. Range 0-15.

username sshkey file

M4250

M4350

This command configures the SSH public key file for a user. The public key file must be entered by a user to encrypt messages with a remote server.

Format	<code>username name sshkey file filename</code>

Mode	Global Config

Parameter	Description
<i>name</i>	The name of the user. The range is from 1 to 64 characters.
<i>filename</i>	The name of the SSH public key file.

no username sshkey file

This command removes the SSH public key file for a user.

Format	<code>no username name sshkey file</code>

Mode	Global Config

username unlock

M4250

M4350

This command allows a locked user account to be unlocked. Only a user with read/write access can reactivate a locked user account.

Format	<code>username name unlock</code>

Mode	Global Config

show users

M4250**M4350**

This command displays the configured user names and their settings. The **show users** command displays truncated user names. Use the **show users long** command to display the complete usernames. The **show users** command is only available for users with read/write privileges. The SNMPv3 fields are displayed only if SNMP is available on the system.

Format	show users
Mode	Privileged EXEC

Term	Definition
User Name	The name the user enters to login using the serial port, Telnet or Web.
Access Mode	Shows whether the user is able to change parameters on the switch (Read/Write) or is only able to view them (Read Only). As a factory default, the “admin” user has Read/Write access and the “guest” has Read Only access.
SNMPv3 Access Mode	The SNMPv3 Access Mode. If the value is set to ReadWrite, the SNMPv3 user is able to set and retrieve parameters on the system. If the value is set to ReadOnly, the SNMPv3 user is only able to retrieve parameter information. The SNMPv3 access mode may be different than the CLI and Web access mode.
SNMPv3 Authentication	The authentication protocol to be used for the specified login user.
SNMPv3 Encryption	The encryption protocol to be used for the specified login user.

show users long

M4250**M4350**

This command displays the complete user names of the configured users on the switch.

Format	show users long
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show users long
User Name
-----
admin
guest
test1111test1111test1111test1111
```

show users accounts

M4250

M4350

This command displays the local user status with respect to user account lockout and password aging. This command displays truncated user names. Use the **show users long** command to display the complete user names.

Format	show users accounts [detail]
Mode	Privileged EXEC
Term	Definition
User Name	The local user account's user name.
Access Level	The user's access level (1 for read-only or 15 for read/write).
Password Aging	Number of days, since the password was configured, until the password expires.
Password Expiry Date	The current password expiration date in date format.
Lockout	Indicates whether the user account is locked out (true or false).

If the detail keyword is included, the following additional fields display.

Term	Definition
Password Override Complexity Check	Displays the user's Password override complexity check status. By default it is disabled.
Password Strength	Displays the user password's strength (Strong or Weak). This field is displayed only if the Password Strength feature is enabled.

Command example:

The following example displays information about the local user database.

```
(NETGEAR Switch)#show users accounts
```

```

UserName           Privilege Password Password    Lockout
                  Aging      Expiry date
-----
admin              15        ---        ---        False
guest              1         ---        ---        False

```

```
console#show users accounts detail
```

```

UserName..... admin
Privilege..... 15
Password Aging..... ---

```

```
Password Expiry..... ---
Lockout..... False
Override Complexity Check..... Disable
Password Strength..... ---
```

```
UserName..... guest
Privilege..... 1
Password Aging..... ---
Password Expiry..... ---
Lockout..... False
Override Complexity Check..... Disable
Password Strength..... ---
```

show users login-history [long]

M4250

M4350

Use this command to display information about the login history of users.

Format	show users login-history [long]

Mode	Privileged EXEC

show users login-history

M4250

M4350

Use this command to display information about the login history of users.

Format	show users login-history [username <i>name</i>]

Mode	Privileged EXEC

Parameter	Description
name	Name of the user. Range: 1-20 characters.

Command example:

The following example shows user login history outputs:

```
Console>show users login-history
Login Time      Username  Protocol  Location
-----
Jan 19 2005 08:23:48 Bob       Serial
Jan 19 2005 08:29:29 Robert    HTTP      172.16.0.8
Jan 19 2005 08:42:31 John      SSH       172.16.0.1
```

Jan 19 2005 08:49:52 Betty Telnet 172.16.1.7

login authentication (Line Config)

M4250

M4350

Use this command to specify the login authentication method list for a line (console, telnet, or SSH). The default configuration uses the default set with the command **aaa authentication login**.

Access the Line Config mode by entering the **line console** command in Global Config mode.

Format	<code>login authentication {default list-name}</code>
Mode	Line Config
Parameter	Description
default	Uses the default list created with the aaa authentication login command.
list-name	Uses the indicated list created with the aaa authentication login command.

Command example:

The following example specifies the default authentication method for a console:

```
(NETGEAR Switch) (config)# line console
(NETGEAR Switch) (config-line)# login authentication default
```

no login authentication

Use this command to return to the default specified by the **authentication login** command.

Format	<code>no login authentication {default list-name}</code>
Mode	Line Config

password (Line Config)

M4250

M4350

Use the **password** command in Line Config, Telnet Config, or SSH Config mode to specify a password on a line, or allow it to be copied from a script file or configuration file. The default configuration is that no password is specified.

Script files or configuration files with password commands that include plain text passwords do not work.

- Access the Line Config mode by entering the **line console** command from the Global Config mode.
- Access the SSH Config mode by entering the **line ssh** command from the Global Config mode.
- Access the Telnet Config mode by entering the **line telnet** command from the Global Config mode.

Format	<code>password [encryption-type encryption-type] password [encryption-type encryption-type] [encrypted]</code>

Mode	Line Config SSH Config Telnet Config

Parameter	Definition
password	The password in encrypted format.
encrypted	The password that is entered or copied from another switch configuration is already encrypted. For SHA-256 salted hash, the password must be 63 characters in length. For SHA-512 salted hash (the default), the password must be 106 characters in length.
encryption-type	The encryption algorithm type, which can be SHA-512 (the default) or SHA-256.

Command example:

The following example configures a plain text password with the SHA-256 encryption type on a line:

```
(NETGEAR Switch) (Config-line) #password encryption-type sha256
Enter new password:*****
Confirm new password:*****
```

Command example:

The following example configures a plain text password with the SHA-512 encryption type on a line:

```
(NETGEAR Switch) (Config-line) #password encryption-type sha512
Enter new password:*****
Confirm new password:*****
```

Command example:

The following example configures an encrypted password with the SHA-256 encryption type on a line:

```
(NETGEAR Switch) (Config-line) #password
$5$8XLN8qHQLKvx61X8$vsIiv0ZqnesHqX/F5yeche4laH4B9WChxyRh5b3vGPB encryption-type sha256
encrypted
```

Command example:

The following example configures an encrypted password with the SHA-512 encryption type on a line:

```
(NETGEAR Switch) (Config-line) #password
$6$iiOcwXwa96ZKoa1F$P6Nj1lVODkH5suf8ic90gj2FJ34EgiK1skJGt3nLevA6C6HJSBxNV0gtz.4DktM/SmE
NiIGFzqkdvhBgX8EGF/ encryption-type sha512 encrypted
```

no password (Line Config)

Use this command to remove the password from a configuration in Line Config, SSH Config, or Telnet Config mode.

Format	no password
Mode	Line Config SSH Config Telnet Config

password (User EXEC)

M4250

M4350

This command allows a user to change the password. The user must enter this command after the password has aged. The user is prompted to enter the old password and the new password.

Format	password
Mode	User EXEC

Command example:

The following example shows the prompt sequence for executing the password command:

```
(NETGEAR Switch)>password
Enter old password:*****
Enter new password:*****
Confirm new password:*****
```

enable password (Privileged EXEC)

M4250

M4350

Use the **enable password** configuration command to set a local password to control access to the privileged EXEC mode.

Script files or configuration files with password commands that include plain text passwords do not work.

Note: When you configure a user password, the password does not display in clear text.

Format	<code>enable password [encryption-type <i>encryption-type</i>] [<i>password</i> [encryption-type <i>encryption-type</i>] [encrypted]]</code>

Mode	Privileged EXEC

Parameter	Description
encryption-type	The encryption algorithm type, which can be SHA-512 (the default) or SHA-256.
password	The password in encrypted format.
encrypted	The password that is entered or copied from another switch configuration is already encrypted. For SHA-256 salted hash, the password must be 63 characters in length. For SHA-512 salted hash (the default), the password must be 106 characters in length.

Command example:

The following example configures a plain text password with the SHA-256 encryption type:

```
(NETGEAR Switch)#enable password encryption-type sha256
Enter old password:*****
Enter new password:*****
Confirm new password:*****
```

Command example:

The following example configures a plain text password with the SHA-512 encryption type:

```
(NETGEAR Switch)#enable password encryption-type sha512
Enter old password:*****
Enter new password:*****
Confirm new password:*****
```

Command example:

The following example configures an encrypted password with the SHA-256 encryption:

```
(NETGEAR Switch)#enable password
$5$8XLN8qHQLKvx61X8$vsIiv0ZqnesHqX/F5yeche4laH4B9WChxyRh5b3vGPB encryption-type sha256
encrypted
```

Command example:

The following example configures an encrypted password with the SHA-512 encryption type:

```
(NETGEAR Switch)#enable password
$6$Zhe76BxSM7ZO8/.$acXOoNVZMbXJuG/L7Ilcfd5iLHL7dd8Gt79bpQacL6UBSdD4GvEudGgP/eaT/wW.Xu
wT3j0o9qKFgLhGZoXz/ encryption-type sha512 encrypted
```

no enable password (Privileged EXEC)

M4250**M4350**

Use the **no enable password** command to remove the password requirement.

Format	no enable password

Mode	Privileged EXEC

passwords min-length

M4250**M4350**

Use this command to enforce a minimum password length for local users. The value also applies to the enable password. The *length* argument is a number in the range 8–64.

Default	8

Format	passwords min-length <i>length</i>

Mode	Global Config

no passwords min-length

Use this command to set the minimum password length to the default value.

Format	no passwords min-length

Mode	Global Config

passwords history

M4250**M4350**

Use this command to set the number of previous passwords that can be stored for each user account. When a local user changes his or her password, the user is not be able to reuse any password stored in password history. This ensures that users do not reuse their passwords often. The number argument is a number in the range 0–10.

Default	0
Format	<code>passwords history number</code>
Mode	Global Config

no passwords history

Use this command to set the password history to the default value.

Format	<code>no passwords history</code>
Mode	Global Config

passwords aging

M4250

M4350

Use this command to implement aging on passwords for local users. When a user's password expires, the user is prompted to change it before logging in again. The *days* argument is a number in the range 1–365 days. The default is 0, or no aging.

Default	0
Format	<code>passwords aging days</code>
Mode	Global Config

no passwords aging

Use this command to set the password aging to the default value.

Format	<code>no passwords aging</code>
Mode	Global Config

passwords lock-out

M4250

M4350

Use this command to strengthen the security of the switch by locking user accounts that have failed login due to wrong passwords. When a lockout count is configured, a user that is logged in must enter the correct password within that count. Otherwise the user will be locked out from further switch access. Only a user with read/write access can reactivate a locked user account. Password lockout does not apply to logins from the serial console. The *number* argument is a number in the range 1–5. The default is 0, or no lockout count enforced.

Default	0
Format	<code>passwords lock-out <i>number</i></code>
Mode	Global Config

no passwords lock-out

Use this command to set the password lock-out count to the default value.

Format	<code>no passwords lock-out</code>
Mode	Global Config

passwords strength-check

M4250

M4350

Use this command to enable the password strength feature. It is used to verify the strength of a password during configuration.

Default	Disable
Format	<code>passwords strength-check</code>
Mode	Global Config

no passwords strength-check

Use this command to set the password strength checking to the default value.

Format	<code>no passwords strength-check</code>
Mode	Global Config

passwords strength maximum consecutive-characters

M4250**M4350**

Use this command to set the maximum number of consecutive characters to be used in password strength. The *number* argument is a number in the range 0–15. The default is 0. Minimum of 0 means no restriction on that set of characters.

Default	0
Format	passwords strength maximum consecutive-characters <i>number</i>
Mode	Global Config

passwords strength maximum repeated-characters

M4250**M4350**

Use this command to set the maximum number of repeated characters to be used in password strength. The *number* argument is a number in the range 0–15. The default is 0. Minimum of 0 means no restriction on that set of characters.

Default	0
Format	passwords strength maximum repeated-characters <i>number</i>
Mode	Global Config

passwords strength minimum uppercase-letters

M4250**M4350**

Use this command to enforce a minimum number of uppercase letters that a password should contain. The *number* argument is a number in the range 0–16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default	2
Format	passwords strength minimum uppercase-letters <i>number</i>
Mode	Global Config

no passwords strength minimum uppercase-letters

Use this command to reset the minimum uppercase letters required in a password to the default value.

Format	no passwords minimum uppercase-letter
Mode	Global Config

passwords strength minimum lowercase-letters

M4250

M4350

Use this command to enforce a minimum number of lowercase letters that a password should contain. The *number* argument is a number in the range 0–16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default	2
Format	passwords strength minimum lowercase-letters <i>number</i>
Mode	Global Config

no passwords strength minimum lowercase-letters

Use this command to reset the minimum lower letters required in a password to the default value.

Format	no passwords minimum lowercase-letter
Mode	Global Config

passwords strength minimum numeric-characters

M4250

M4350

Use this command to enforce a minimum number of numeric characters that a password should contain. The *number* argument is a number in the range 0–16. T The default is 2. Minimum of 0 means no restriction on that set of characters.

Default	2
Format	passwords strength minimum numeric-characters <i>number</i>
Mode	Global Config

no passwords strength minimum numeric-characters

Use this command to reset the minimum numeric characters required in a password to the default value.

Format	no passwords strength minimum numeric-characters

Mode	Global Config

passwords strength minimum special-characters

M4250

M4350

Use this command to enforce a minimum number of special characters that a password should contain. The *number* argument is a number in the range 0–16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default	2

Format	passwords strength minimum special-characters <i>number</i>

Mode	Global Config

no passwords strength minimum special-characters

Use this command to reset the minimum special characters required in a password to the default value.

Format	no passwords strength minimum special-characters

Mode	Global Config

passwords strength minimum character-classes

Use this command to enforce a minimum number of characters classes that a password should contain. Character classes are uppercase letters, lowercase letters, numeric characters and special characters. The *number* argument is a number in the range 0–4. The default is 4.

Default	4

Format	passwords strength minimum character-classes <i>number</i>

Mode	Global Config

no passwords strength minimum character-classes

Use this command to reset the minimum number of character classes required in a password to the default value.

Format	no passwords minimum character-classes
Mode	Global Config

passwords strength exclude-keyword

M4250

M4350

Use this command to exclude the specified keyword while configuring the password. The password does not accept the keyword in any form (in between the string, case in-sensitive and reverse) as a substring. You can configure up to a maximum of three keywords.

Format	passwords strength exclude-keyword <i>keyword</i>
Mode	Global Config

no passwords strength exclude-keyword

Use this command to reset the restriction for the specified keyword or all the keywords configured.

Format	no passwords exclude-keyword [<i>keyword</i>]
Mode	Global Config

passwords unlock timer

M4250

M4350

Use this command to configure the time after which a locked user account is unlocked (that is, the unlock time) and password authentication can be attempted again. By default, the period for the *minutes* argument is 5 minutes and the range is from 1 to 60 minutes.

Default	5
Format	passwords unlock timer <i>minutes</i>
Mode	Global Config

no passwords unlock timer

Use this command to reset the unlock time to the default time.

Format	no passwords unlock timer

Mode	Global Config

passwords unlock timer mode

M4250

M4350

Use this command to configure the password unlock timer mode. If the user account is locked, the timer mode is enabled (which it is by default), and the unlock time expires, the user account is unlocked. If the timer mode is disabled and the unlock time expires, the user account remains locked.

Default	Enabled

Format	passwords unlock timer mode {enabled disabled}

Mode	Global Config

no passwords unlock timer mode

Use this command to reset the unlock timer mode to its default.

Format	no passwords unlock timer mode

Mode	Global Config

show passwords configuration

M4250

M4350

Use this command to display the configured password management settings.

Format	show passwords configuration

Mode	Privileged EXEC

Term	Definition
Minimum Password Length	The minimum number of characters that the password must include.
Password Aging (day)	The length in days that a password is valid.
Password History	The number of passwords to store for reuse prevention.
Lockout Attempts	The number of failed password login attempts allowed before lockout occurs.

Term	Definition
Password Strength Check	Indicates if the password strength check is enabled.
Minimum Password Uppercase Letters	The minimum number of uppercase characters that the password must include.
Minimum Password Lowercase Letters	The minimum number of lowercase characters that the password must include.
Minimum Password Numeric Characters	The minimum number of numeric characters that the password must include.
Minimum Password Special Characters	The minimum number of special characters that the password must include.
Maximum Password Repeated Characters	The maximum number of repeated characters that the password can include.
Maximum Password Consecutive Characters	The maximum number of consecutive repeated characters that the password can include.
Minimum Password Character Classes	The minimum number of character classes (uppercase, lowercase, numeric and special) that the password must include.
Password Exclude-Keywords	The set of keywords to be excluded from the configured password when strength checking is enabled.
Unlock Timer Mode	Indicates if the unlock timer mode is enabled.
Unlock Time (mins)	The time after which a locked user account is unlocked

show passwords result

M4250

M4350

Use this command to display the last password set result information.

Format	<code>show passwords result</code>
Mode	Privileged EXEC

Term	Definition
Last User Whose Password Is Set	Shows the name of the user with the most recently set password.
Password Strength Check	Shows whether password strength checking is enabled.
Last Password Set Result	Shows whether the attempt to set a password was successful. If the attempt failed, the reason for the failure is included.

aaa ias-user username

M4250

M4350

The Internal Authentication Server (IAS) database is a dedicated internal database used for local authentication of users for network access through the IEEE 802.1X feature.

Use the **aaa ias-user username** command in Global Config mode to add the specified user to the internal user database. This command also changes the mode to AAA User Config mode.

Format	<code>aaa ias-user username user</code>
Mode	Global Config

no aaa ias-user username

Use this command to remove the specified user from the internal user database.

Format	<code>no aaa ias-user username user</code>
Mode	Global Config

Command example:

```
(NETGEAR Switch) #
(NETGEAR Switch) #configure
(NETGEAR Switch) (Config)#aaa ias-user username client-1
((NETGEAR Switch) (Config-aaa-ias-User)#exit
(NETGEAR Switch) (Config)#no aaa ias-user username client-1
(NETGEAR Switch) (Config)#
```

aaa session-id

M4250

M4350

Use this command in Global Config mode to specify if the same session-id is used for Authentication, Authorization and Accounting service type within a session.

Default	common
Format	<code>aaa session-id [common unique]</code>
Mode	Global Config

Parameter	Description
common	Use the same session-id for all AAA Service types.
unique	Use a unique session-id for all AAA Service types.

no aaa session-id

Use this command in Global Config mode to reset the aaa session-id behavior to the default.

Format	no aaa session-id [unique]
Mode	Global Config

aaa accounting

M4250

M4350

Use this command in Global Config mode to create an accounting method list for user EXEC sessions, user-executed commands, or DOT1X. This list is identified by the **default** keyword or by a user-specified *list-name*. Accounting records, when enabled for a line-mode, can be sent at both the beginning and at the end (**start-stop**) or only at the end (**stop-only**). If **none** is specified, accounting is disabled for the specified list. If **tacacs** is specified as the accounting method, accounting records are notified to a TACACS+ server. If **radius** is the specified accounting method, accounting records are notified to a RADIUS server.

Note the following:

- A maximum of five Accounting Method lists can be created for each exec and commands type.
- Only the default Accounting Method list can be created for DOT1X. There is no provision to create more.
- The same list-name can be used for both exec and commands accounting type
- AAA Accounting for commands with RADIUS as the accounting method is not supported.
- Start-stop or None are the only supported record types for DOT1X accounting. Start-stop enables accounting and None disables accounting.
- RADIUS is the only accounting method type supported for DOT1X accounting.

Format	aaa accounting {exec commands dot1x} {default <i>list-name</i> } {start-stop stop-only none} <i>method1</i> [<i>method2...</i>]
Mode	Global Config

Parameter	Description
exec	Provides accounting for a user EXEC terminal sessions.
commands	Provides accounting for all user executed commands.
dot1x	Provides accounting for DOT1X user commands.
default	The default list of methods for accounting services.
list-name	Character string used to name the list of accounting methods.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the beginning of a process and a stop accounting notice at the end of a process.
stop-only	Sends a stop accounting notice at the end of the requested user process.
none	Disables accounting services on this line.
method	Use either TACACS or radius server for accounting purposes.

Command example:

```
(NETGEAR Switch) #
(NETGEAR Switch) #configure
(NETGEAR Switch) #aaa accounting commands default stop-only tacacs
(NETGEAR Switch) #aaa accounting exec default start-stop radius
(NETGEAR Switch) #aaa accounting dot1x default start-stop radius
(NETGEAR Switch) #aaa accounting dot1x default none
(NETGEAR Switch) #exit
```

Command example:

For the same set of accounting type and list name, the administrator can change the record type, or the methods list, without having to first delete the previous configuration:

```
(NETGEAR Switch) #
(NETGEAR Switch) #configure
(NETGEAR Switch) #aaa accounting exec ExecList stop-only tacacs
(NETGEAR Switch) #aaa accounting exec ExecList start-stop tacacs
(NETGEAR Switch) #aaa accounting exec ExecList start-stop tacacs radius
```

The first **aaa** command creates a method list for exec sessions with the name `ExecList`, with record-type as **stop-only** and the method as **tacacs**. The second command changes the record type from **stop-only** to **start-stop** for the same method list. The third command, for the same list changes the methods list from **tacacs** to **tacacs ,radius**.

no aaa accounting

This command deletes the accounting method list.

Format	no aaa accounting {exec commands dot1x} {default <i>list-name</i> }
Mode	Global Config

Command example:

```
(NETGEAR Switch) #
(NETGEAR Switch) #configure
(NETGEAR Switch) #aaa accounting commands userCmdAudit stop-only tacacs radius
(NETGEAR Switch) #no aaa accounting commands userCmdAudit
(NETGEAR Switch) #exit
```

aaa accounting update

M4250

M4350

Use this command to send interim accounting records to the accounting server or to configure how often new or interim accounting records must be sent to the accounting server.

Default	newinfo: Disabled Periodic: 5 minutes
Format	aaa accounting update [newinfo [periodic 1-200] periodic 1-200]]
Mode	Global Config
Parameter	Definition
newinfo	Updates are sent to the RADIUS server whenever there is a new information available, such as reauthentication of a client.
periodic	The interval at which interim accounting records are sent, in minutes

Command example:

```
(NETGEAR Switch) #(Config)#aaa accounting update newinfo periodic 20
```

no aaa accounting update

This command resets sending the interim accounting records to the default values.

Format	no aaa accounting update
Mode	Global Config

password (AAA IAS User Config)

M4250**M4350**

Use this command to specify a password for a user in the IAS database. You can also use the **encrypted** keyword to enter the password in encrypted format (32 characters in hexadecimal format).

Format	password { <i>password</i> encrypted <i>password</i> }
Mode	AAA IAS User Config
Parameter	Definition
password	Password for this level. Range: 8-64 characters

Command example:

```
(NETGEAR Switch) #
(NETGEAR Switch) #configure
(NETGEAR Switch) (Config)#aaa ias-user username client-1
(NETGEAR Switch) (Config-aaa-ias-User)#password client123
(NETGEAR Switch) (Config-aaa-ias-User)#no password
```

Command example:

The following is an example of adding a MAB Client to the Internal user database:

```
(NETGEAR Switch) #
(NETGEAR Switch) #configure
(NETGEAR Switch) (Config)#aaa ias-user username 1f3ccb1157
(NETGEAR Switch) (Config-aaa-ias-User)#password 1f3ccb1157
(NETGEAR Switch) (Config-aaa-ias-User)#exit
(NETGEAR Switch) (Config)#
```

no password (AAA IAS User Config)

Use this command to clear the password of a user.

Format	no password
Mode	AAA IAS User Config

clear aaa ias-users

M4250

M4350

Use this command to remove all users from the IAS database.

Format	clear aaa ias-users

Mode	Privileged Exec

Command example:

```
(NETGEAR Switch) #clear aaa ias-users
```

show aaa ias-users

M4250

M4350

Use this command to display configured IAS users and their attributes. Passwords configured are not shown in the show command output.

Format	show aaa ias-users [username]

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show aaa ias-users
```

```
UserName
```

```
-----
```

```
Client-1
```

```
Client-2
```

Following are the IAS configuration commands shown in the output of **show running-config** command. Passwords shown in the command output are always encrypted.

```
aaa ias-user username client-1
password a45c74fdf50a558a2b5cf05573cd633bac2c6c598d54497ad4c46104918f2c encrypted
exit
```

accounting

M4250

M4350

Use this command to apply an accounting method list to a configuration in Line Config, SSH Config, or Telnet Config mode.

- Access the Line Config mode by entering the **line console** command from the Global Config mode.
- Access the SSH Config mode by entering the **line ssh** command from the Global Config mode.
- Access the Telnet Config mode by entering the **line telnet** command from the Global Config mode.

Format	<code>accounting {exec commands} {default list-name}</code>
Mode	Line Config SSH Config Telnet Config
Parameter	Description
exec	Causes accounting for an EXEC session.
commands	This causes accounting for each command execution attempt. If a user is enabling accounting for exec mode for the current line-configuration type, the user will be logged out.
default	The default Accounting List
listname	Enter a string of not more than 15 characters.

Command example:

```
(NETGEAR Switch) #
(NETGEAR Switch) #configure
(NETGEAR Switch) (Config)#line telnet
(NETGEAR Switch) (Config-line)# accounting exec default
(NETGEAR Switch) #exit
```

no accounting

Use this command to remove accounting from a configuration in Line Config, SSH Config, or Telnet Config mode.

Format	<code>no accounting {exec commands}</code>
Mode	Line Config SSH Config Telnet Config

show accounting

M4250

M4350

Use this command to display ordered methods for accounting lists.

Format	show accounting

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show accounting
Number of Accounting Notifications sent at beginning of an EXEC session:      0
Errors when sending Accounting Notifications beginning of an EXEC session:    0
Number of Accounting Notifications at end of an EXEC session:                 0
Errors when sending Accounting Notifications at end of an EXEC session:        0
Number of Accounting Notifications sent at beginning of a command execution:   0
Errors when sending Accounting Notifications at beginning of a command execution: 0
Number of Accounting Notifications sent at end of a command execution:         0
Errors when sending Accounting Notifications at end of a command execution:     0
```

show accounting methods

M4250

M4350

Use this command to display configured accounting method lists.

Format	show accounting methods

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #
(NETGEAR Switch) #show accounting methods
```

Acct Type	Method Name	Record Type	Method Type
-----	-----	-----	-----
Exec	dfltExecList	start-stop	TACACS
Commands	dfltCmdsList	stop-only	TACACS
Commands	UserCmdAudit	start-stop	TACACS
DOT1X	dfltDot1xList	start-stop	radius

Line	EXEC Method List	Command Method List
-----	-----	-----
Console	dfltExecList	dfltCmdsList

Telnet	dfltExecList	dfltCmdsList
SSH	dfltExecList	UserCmdAudit

show accounting update

M4250

M4350

Use this command to display the accounting interim update information.

Format	show accounting update

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show accounting update
```

```
aaa accounting  update newinfo  : Enabled
aaa accounting  update periodic : 10 minutes
```

clear accounting statistics

M4250

M4350

This command clears the accounting statistics.

Format	clear accounting statistics

Mode	Privileged Exec

show domain-name

M4250

M4350

This command displays the configured domain-name.

Format	show domain-name

Mode	Privileged Exec

Command example:

```
(NETGEAR Switch) #show domain-name
```

```
Domain           : Enable
Domain-name      : abc
```

SNMP Commands

This section describes the commands that you can use to configure Simple Network Management Protocol (SNMP) on the switch. You can configure the switch to act as an SNMP agent so that it can communicate with SNMP managers on your network.

snmp-server

M4250

M4350

This command sets the name and the physical location of the switch and the organization responsible for the network. The range for the *name*, *loc* and *con* parameters is from 1 to 31 alphanumeric characters.

Default	none
Format	snmp-server {sysname <i>name</i> location <i>loc</i> contact <i>con</i> }
Mode	Global Config

snmp-server engineid local

M4250

M4350

This command changes the SNMPv3 engine ID on the switch. By default, the SNMP engine ID is based on the MAC address of the switch.

Note: If you change the SNMP engine ID, any existing SNMP configuration is deleted and you must reconfigure the SNMP configuration on the switch.

Default	default
Format	snmp-server engineid local { <i>engineid-string</i> default}
Mode	Global Config

Parameter	Description
engineid-string	The custom SNMPv3 engine ID (from 6 to 32 characters).
default	The SNMPv3 engine ID is based on the MAC address of the switch.

no snmp-server engineid local

This command removes a custom SNMP engine ID.

Note: If you remove a custom SNMP engine ID, any existing SNMP configuration is deleted and you must reconfigure the SNMP configuration on the switch.

Format	<code>no snmp-server engineid local</code>

Mode	Global Config

snmp-server community

M4250

M4350

This command adds (and names) a new SNMPv1 or SNMPv2 community. A community name is associated with the switch and with a set of SNMP managers that manage the community with a specified privileged level. Community names in the SNMP community table must be unique. If multiple entries are made using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

Format	<code>snmp-server community <i>community-string</i> [ipaddress {<i>ipaddress</i> [<i>ipmask</i>] <i>prefix/prefix-length</i>}] [ro rw su] [view <i>view-name</i>]</code>

Mode	Global Config

Parameter	Description
community-string	The name (from 1 to 30 characters) of the new community.
ro	The community receives read-only privileges, which lets a user view but not change any object values.
rw	The community receives read and write privileges, which lets a user both view and change all object values.
su	The community receives super user (administrator) privileges, which lets a user configure the switch.
view-name	The name of the view (from 1 to 30 characters) to which the community is limited.
ipaddress ipaddress	The IPv4 address from which the community is allowed access. The SNMP community sends SNMP packets from this address. The address along with the client IP mask value denotes a range of IP addresses from which SNMP clients can use the community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses.

Parameter	Description
ipmask	The optional client IP mask for an SNMP community. The SNMP community sends SNMP packets from an address with this client IP mask. The address along with the client IP mask value denotes a range of IP addresses from which SNMP clients can use the community to access the device. A value of 255.255.255.255 allows access from only one computer and specifies that computer's IP address as the client IP address. A value of 0.0.0.0 allows access from any IP address.
ipaddress <i>prefix/prefix-length</i>	The IPv6 address from which the community is allowed access. The SNMP community sends SNMP packets from this address.

no snmp-server community

This command removes an SNMPv1 or SNVP2 community that you specify by entering the community string.

Format `no snmp-server community community-string`

Mode Global Config

snmp-server community-group

M4250

M4350

This command configures a community access string to permit access through the SNMPv1 and SNMPv2 protocols.

Format `snmp-server community-group community-string group-name [ipaddress ipaddress]`

Mode Global Config

Parameter	Description
community-string	The name of the community access string (from 1 to 20 characters) that becomes associated with the community group.
group-name	The name of the community group (from 1 to 30 characters) with which the community access string must be associated.
ipaddress	The IPv4 or IPv6 address from which the community group is allowed access.

no snmp-server community-group

This command removes a community access string.

Format `no snmp-server community-group community-string`

Mode Global Config

snmp-server host

M4250

M4350

This command configures an SNMPv1 or SNMPv2 host to which the switch can send traps.

Default	No host
Format	<code>snmp-server host {ipaddr ipv6addr hostname} {informs [timeout seconds] [retries retries] traps version {1 2}} community-string [udp-port port] [filter filter-name]</code>
Mode	Global Config
Parameter	Description
ipaddr, ipv6addr, or hostname	The IPv4 or IPv6 address or name of the host.
informs	The switch sends SNMPv2 informs to the host. (The switch sends either informs or traps.)
seconds	The period in seconds (from 1 to 300 seconds) that the switch waits for an acknowledgement before it sends the inform again. This default is 15 seconds.
retries	The number of times (from 0 to 255) that the switch attempts to send the same inform. The default is 3 attempts.
traps	The switch sends traps to the host. (The switch sends either traps or informs.)
1	The switch sends SNMPv1 traps.
2	The switch sends SNMPv2c traps.
community-string	The community string (from 1 to 20 characters) that is sent as part of the notification.
port	The SNMP trap receiver port. By default, the port number is 162, but you can specify another port number.
filter-name	The filter name (from 1 to 30 characters) that is associated with the host. (You can use a filter to specify which traps are sent to the host.)

no snmp-server host

This command removes the traps or informs configuration for an SNMP host.

For information about the parameters, see the **snmp-server host** command.

Format	<code>no snmp-server host {ipaddr ipv6addr hostname} {traps version {1 2} informs}</code>
Mode	Global Config

snmp-server v3-host

M4250

M4350

This command configures an SNMPv3 host to which the switch can send traps.

Default	No host
Format	<code>snmp-server v3-host {ipaddr ipv6addr hostname} username {traps {auth priv} informs {auth priv} [timeout seconds] [retries retries]} [udpport port] [filter filtername]</code>
Mode	Global Config

Parameter	Description
ipaddr, ipv6addr, or hostname	The IPv4 or IPv6 address or name of the host.
username	The name of the user (from 1 to 30 characters). The user must be associated with a group that supports SNMPv3 and the access method that you configure for this command.
traps	The switch sends traps to the host. (The switch sends either traps or informs.)
informs	The switch sends informs to the host. (The switch sends either informs or traps.)
seconds	The period in seconds (from 1 to 300 seconds) that the switch waits for an acknowledgement before it sends the inform again. This default is 15 seconds.
retries	The number of times (from 0 to 255) that the switch attempts to send the same inform. The default is 3 attempts.
auth	Authentication is required but encryption is not required.
noauth	Neither authentication or encryption is required (This is the default setting.)
priv	Both authentication and encryption are required.
port	The SNMPv3 trap receiver port. By default, the port number is 162, but you can specify another port number.
filter-name	The filter name (from 1 to 30 characters) that is associated with the host. (You can use a filter to specify which traps are sent to the host.)

no snmp-server v3-host

This command removes the traps or informs configuration for an SNMPv3 host.

For information about the parameters, see the **snmp-server v3-host** command.

Format	<code>no snmp-server v3-host {ipaddr ipv6addr hostname} {traps informs}</code>
Mode	Global Config

snmp-server group

M4250

M4350

This command creates a custom SNMP access group.

Default	No customs groups, but generic groups exist for all SNMP version and privileges.
Format	<code>snmp-server group <i>group-name</i> {v1 v2 v3 {auth priv}} [notify <i>notify-view</i>] [read <i>read-view</i>] [write <i>write-view</i>]</code>
Mode	Global Config
Parameter	Description
group-name	The group name (from 1 to 30 characters).
v1	This group is allowed access to SNMPv1 only.
v2	This group is allowed access to SNMPv2c only.
v3	This group is allowed access to SNMPv3 only.
auth	The group is allowed access to SNMPv3 only and only when authentication is enabled but encryption is disabled.
priv	The group is allowed access to SNMPv3 only and only when both authentication or encryption are enabled.
read-view	The name of the view (from 1 to 30 characters) that the group can access during GET requests.
write-view	The name of the view (from 1 to 30 characters) that the group can access during SET requests.
notify-view	The name of the view (from 1 to 30 characters) that the group can access when traps are sent.

no snmp-server group

This command removes an SNMP access group.

For information about the parameters, see the **snmp-server group** command.

Format	<code>no snmp-server group <i>group-name</i> {v1 v2 v3 {auth priv}}</code>
Mode	Global Config

snmp-server user

M4250**M4350**

This command creates an SNMPv3 user that can access the switch.

Default	No default user
Format	<code>snmp-server user username groupname [remote {engineid-string address {ipaddr ipv6addr hostname}}] [auth-sha512 authentication-password auth-sha512-key sha512-key] {[priv-aes128 encryption-password priv-aes128-key aes128-key]}</code>
Mode	Global Config

Parameter	Description
username	The name (from 1 to 30 characters) of the SNMPv3 user.
groupname	The group name (from 1 to 30 characters) of which the SNMPv3 user is a member.
engineid-string	The engine-id (from 6 to 32 characters) of the remote management station that this user will be connecting from.
ipaddr, ipv6addr, or hostname	The IPv4 or IPv6 address or name of the remote management station that this user will be connecting from.
auth-sha512	Indicates that you must enter a password on the basis of which the switch can generate an SHA-512 key for authentication.
authentication-password	The actual password (from 1 to 32 characters) that lets the switch automatically generate an SHA-512 key for authentication.
auth-sha512-key	Indicates that you must enter (or copy) the SHA-512 key for authentication.
sha512-key	The actual SHA-512 key for authentication. The key can be up to 128 characters. If you do not enter a key, the switch automatically generates a key.
priv-aes128	Indicates that you must enter a password on the basis of which the switch can generate an AES-128 HMAC-MD5-96 key for encryption.
encryption-password	The actual password (from 1 to 32 characters) that lets the switch automatically generate an AES-128 HMAC-MD5-96 key for encryption.
priv-aes128-key	Indicates that you must enter (or copy) the AES-128 HMAC-MD5-96 key for encryption.
aes128-key	The actual AES-128 HMAC-MD5-96 key for encryption. The key can be up to 128 characters. If you do not enter a key, the switch automatically generates a key.

Command example:

```
(NETGEAR Switch) (Config)#snmp-server user test grp1 auth-sha512 priv-aes128
```

```
Enter Authentication Password:*****
Confirm Authentication Password:*****
Enter Encryption Password:*****
```

Confirm Encryption Password:*****

Command example:

```
(NETGEAR Switch) (Config) #snmp-server user test DefaultWrite auth-sha512-key
6991313bb623241c8f6f967fa28dff0265b4b57dfd07301be41024a791df01f412d1ad8bd8cde6ae6d66da7
61987657afe36efd788d021012564cf8ed2718351 priv-aes128-key
6991313bb623241c8f6f967fa28dff0265b4b57dfd07301be41024a791df01f412d1ad8bd8cde6ae6d66da7
61987657afe36efd788d021012564cf8ed2718351
```

no snmp-server user

This command removes an SNMPv3 user.

Format	no snmp-server user <i>username</i>
Mode	Global Config

snmp-server enable traps

M4250

M4350

This command enables the Authentication Flag.

Default	enabled

Format	snmp-server enable traps

Mode	Global Config

no snmp-server enable traps

This command disables the Authentication Flag.

Format	no snmp-server enable traps

Mode	Global Config

snmp-server enable traps violation

M4250

M4350

This command enables the switch to send violation traps. The switch sends a violation trap if it receives a packet with a disallowed MAC address on a locked port.

Note: For information about port security commands, see [Protected Port Commands](#) on page 603.

Default	disabled

Format	<code>snmp-server enable traps violation</code>

Mode	Global Config

`no snmp-server enable traps violation`

This command prevents the switch from sending violation traps.

Format	<code>no snmp-server enable traps violation</code>

Mode	Global Config

`snmp-server enable traps linkmode`

M4250

M4350

This command enables Link Up/Down traps for the entire switch. If enabled, the switch sends link traps only if the Link Trap flag setting that is associated with a port is enabled. For more information, see [snmp trap link-status](#) on page 176

Default	enabled

Format	<code>snmp-server enable traps linkmode</code>

Mode	Global Config

`no snmp-server enable traps linkmode`

This command disables Link Up/Down traps for the entire switch.

Format	<code>no snmp-server enable traps linkmode</code>

Mode	Global Config

snmp-server enable traps multiusers

M4250

M4350

This command enables multiple user traps. If the traps are enabled, the switch sends a multiple user trap if a user logs in to the terminal interface (EIA 232 or Telnet) while an existing terminal interface session is already established.

Default	enabled
Format	snmp-server enable traps multiusers
Mode	Global Config

no snmp-server enable traps multiusers

This command disables multiple user traps.

Format	no snmp-server enable traps multiusers
Mode	Global Config

snmp-server enable traps stpmode

M4250

M4350

This command enables the switch to send new root traps and topology change notification traps.

Default	enabled
Format	snmp-server enable traps stpmode
Mode	Global Config

no snmp-server enable traps stpmode

This command prevents the switch from sending new root traps and topology change notification traps.

Format	no snmp-server enable traps stpmode
Mode	Global Config

snmp-server enable traps mac-notification change

M4250**M4350**

This command enables MAC notification traps or informs to be sent to the SNMP server. MAC notification traps are sent only when they are enabled on an interface using the **snmp trap mac-notification change** command when the **snmp-server enable traps mac-notification change** command is enabled.

Default	disabled
Format	snmp-server enable traps mac-notification change
Mode	Global Config

no snmp-server enable traps mac-notification change

This command disables MAC notification traps or informs to be sent to the SNMP server.

Format	no snmp-server enable traps mac-notification change
Mode	Global Config

snmp-server enable traps captive-portal

M4250**M4350**

This command enables captive portal traps or informs to be sent to the SNMP server. The specific captive portal traps are configured using the **trapflags** command in Captive Portal Config mode.

Default	disabled
Format	snmp-server enable traps captive-portal
Mode	Global Config

no snmp-server enable traps captive portal

This command disables captive portal traps or informs to be sent to the SNMP server.

Format	no snmp-server enable traps captive-portal
Mode	Global Config

show mac-address-table notification change

M4250**M4350**

This command displays the MAC notification configuration and contents of the MAC notification history table. If you specify an interface, the command displays the status of SNMP trap for MAC notification for that interface.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show mac-address-table notification change [interface <i>unit/slot/port</i>]</code>

Mode	Privileged EXEC

snmp-server filter

M4250**M4350**

This command creates a filter entry that lets you limit which traps are sent to a host.

Default	No filters entries

Format	<code>snmp-server filter <i>filtername</i> <i>oid-tree</i> {included excluded}</code>

Mode	Global Config

Parameter	Description
<i>filtername</i>	The name for the filter (from 1 to 30 characters)
<i>oid-tree</i>	The OID subtree that must be included in or excluded from the filter. You can specify a subtree by numerals (for example, 1.3.6.2.4), keywords (for example, system). You can also use asterisks to specify a subtree family (for example, 1.3.*.4).
<i>included</i>	The subtree must be included in the filter.
<i>excluded</i>	The subtree must be excluded from the filter.

no snmp-server filter

This command removes a filter that you must specify. In addition, you can also specify a subtree.

Format	<code>snmp-server filter <i>filtername</i> [<i>oid-tree</i>]</code>

Mode	Global Config

snmp-server view

M4250**M4350**

This command creates a new view or modifies an existing view that an SNMP group can use to determine which objects can be accessed by a community or user.

Default	The switch automatically creates default view for default groups.
Format	<code>snmp-server view viewname oid-tree {included excluded}</code>
Mode	Global Config
Parameter	Description
viewname	The name for the view (from 1 to 30 characters)
oid-tree	The OID subtree that must be included in or excluded from the view. You can specify a subtree by numerals (for example, 1.3.6.2.4), keywords (for example, system). You can also use asterisks to specify a subtree family (for example, 1.3.*.4).
included	The subtree must be included in the view.
excluded	The subtree must be excluded from the view.

no snmp-server view

This command removes a view that you must specify. In addition, you can also specify a subtree.

Format	<code>snmp-server view viewname [oid-tree]</code>
Mode	Global Config

snmp-server port

M4250**M4350**

This command modifies the port that the switch uses to detect SNMP messages. By default, the switch uses UDP port 161 to detect SNMP messages.

Default	161
Format	<code>snmp-server port number</code>
Mode	Privileged EXEC

no snmp-server port

This command resets the port that the switch uses to detect SNMP messages. After you enter this command, the switch uses UDP port 161 to detect SNMP messages.

Format	no snmp-server port

Mode	Privileged EXEC

snmp-server trapsend

M4250

M4350

Use this command to set the UDP port to which traps are sent by the SNMP server.

Default	50505

Format	snmp-server trapsend <i>number</i>

Mode	Privileged EXEC

no snmp-server trapsend

Use this command to reset the UDP port to which traps are sent by the SNMP server to the default port of 50505.

Format	no snmp-server trapsend

Mode	Privileged EXEC

snmptrap source-interface

M4250

M4350

This command configures the global source interface (that is, the source IP address) for all SNMP communication between the SNMP client and the server.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	snmptrap source-interface { <i>unit/slot/port</i> loopback <i>loopback-id</i> serviceport vlan <i>vlan-id</i> }

Mode	Global Config

Parameter	Description
unit/slot/port	The unit identifier that is assigned to the switch.
loopback-id	The loopback interface that you want to use as the source IP address. The range of the loopback ID is from 0 to 7.
serviceport	The service port IP address is used.
vlan-id	The VLAN interface that you want to use as the source IP address. The range of the VLAN ID is from 1 to 4093.

no snmptrap source-interface

This command removes the global source interface for all SNMP communication between the SNMP client and the server.

Format	no snmptrap source-interface
Mode	Global Config

snmp trap link-status

M4250

M4350

This command enables link status traps for an interface or for all interfaces.

Format	snmp trap link-status
Mode	Interface Config

no snmp trap link-status

This command disables link status traps for an interface.

Format	no snmp trap link-status
Mode	Interface Config

snmp trap link-status all

M4250

M4350

This command enables link status traps for all interfaces.

Format	snmp trap link-status all
Mode	Global Config

no snmp trap link-status

This command disables link status traps for all interfaces.

Format	no snmp trap link-status all

Mode	Global Config

snmp trap mac-notification change

M4250

M4350

This command enables MAC notification traps to be sent for an interface.

The **added** keyword causes a trap to be sent when an interface is added. The **removed** keyword causes a trap to be sent when an interface is removed. You can configure both keywords, one after the other.

Format	snmp trap mac-notification change [added removed]

Mode	Interface Config

no snmp trap mac-notification change

This command disables MAC notification traps to be sent for an interface.

The **added** keyword stops a trap from being sent when an interface is added. The **removed** keyword stops a trap from being sent when an interface is removed. You can configure both keywords, one after the other.

Format	no snmp trap mac-notification change [added removed]

Mode	Interface Config

show snmp-server

M4250

M4350

This command shows the UDP port to which the SNMP server is connected and on which the switch sends SNMP traps.

Format	show snmp-server

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch)#show snmp-server
SNMP Server Port..... 161
SNMP Trap Send Port..... 162
```

show snmp engineID

M4250

M4350

This command displays the configured SNMP engine ID.

Format	show snmp engineID

Mode	Privileged EXEC

show snmp

M4250

M4350

This command displays the SNMP configuration on the switch.

Format	show snmp

Mode	Privileged EXEC

Term	Definition
Community tables	
Community-String	The community string for the entry. The community string is used by the SNMPv1 and SNMPv2 protocols to access the switch.
Community-Access	The privilege level: Read only, Read write, or su (which means super user).
View Name	The name of the view to which the community receives access.
IP Address	The IP address from which access to the community is allowed.
IP Mask	The IP mask associated with the IP address.
Community Group tables	
Community-String	The community string for the entry. The community string is used by the SNMPv1 and SNMPv2 protocols to access the switch.
Group Name	The group to which the community is assigned.
IP Address	The IP address from which the group can access the community
IP Mask	The IP mask associated with the IP address.
Host table for SNMPv1 and SNMPv2	
Target Address	The IP address of the host to which SNMPv1 or SNMPv2 traps or informs are sent.
Type	The type of SNMPv1 or SNMPv2 messages that are sent (either traps or informs).
Community	The community to which the SNMPv1 or SNMPv2 messages are sent.

Term	Definition
Version	The SNMP version (SNMPv1 or SNMPv2) of the messages.
UDP Port	The number of the UDP port to which the SNMPv1 or SNMPv2 messages are sent.
Filter Name	The name of the filter that limits the SNMPv1 or SNMPv2 messages for the host.
TO sec	The period in seconds before SNMPv1 or SNMPv2 inform messages time out.
Retries	The number of times that the switch attempts to send the same SNMPv1 or SNMPv2 inform message.

Host table for SNMPv3

Target Address	The IP address of the host to which SNMPv3 traps or informs are sent.
Type	The type of SNMPv3 messages that are sent (either traps or informs).
User Name	The name of the SNMPv3 user to which access is granted.
Security Level	The privilege level that is assigned to the SNMPv3 user.
UDP Port	The number of the UDP port to which the SNMPv3 messages are sent.
Filter Name	The name of the filter that limits the SNMPv3 messages for the host.
TO sec	The period in seconds before SNMPv3 inform messages time out.
Retries	The number of times that the switch attempts to send the same SNMPv3 inform message.

show snmp filters

M4250**M4350**

This command displays either all filters that are used when SNMP messages are sent or a specific filter that you must enter.

Format `show snmp filters [filtername]`

Mode Privileged EXEC

Term	Definition
Name	The name of the filter.
OID Tree	The name of the OID subtree.
Type	Shows if the OID tree is included in or excluded from the filter.

show snmp group

M4250

M4350

This command displays either all SNMP groups or a specific SNMP group that you must enter.

Format	<code>show snmp group [groupname]</code>
Mode	Privileged EXEC
Term	Definition
Name	The name of the group.
Context Prefix	The name of the context that is associated with the group.
Security Model	The protocol that can access the switch through the group.
Security Level	The security level that is allowed for the group.
Views Read	The view that this group provides read-access to.
Views Write	The view that this group provides write-access to.
Views Notify	The view that this group provides trap-access to.

show snmp user

M4250

M4350

This command displays either all SNMPv3 users or a specific SNMPv3 user that you must enter.

Format	<code>show snmp user [username]</code>
Mode	Privileged EXEC
Term	Definition
Name	The name of the user.
Group Name	The name of the group to which the user is assigned and that defines the SNMPv3 settings.
Auth Meth	The authentication method for the user.
Priv Meth	The encryption method for the user.
Remote Engine ID	The SNMP engine ID for the user device.

show snmp views

M4250

M4350

This command displays either all SNMP views or a specific SNMP view that you must enter.

Format	show snmp views [viewname]
Mode	Privileged EXEC
Term	Definition
Name	The name of the view.
OID Tree	The name of the OID subtree.
Type	Shows if the OID tree is included in or excluded from the view.

show trapflags (M4250 series switch)

M4250

This command displays the trap conditions. The command output shows all enabled trap flags.

Note: You can configure which traps the switch must generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the SNMP agent on the switch sends the trap to all enabled trap receivers. Cold and warm start traps are always generated and cannot be disabled.

Format	show trapflags
Mode	Privileged EXEC
Term	Definition
Authentication Flag	Indicates if an authentication failure trap is sent. By default, the flag is enabled.
Link Up/Down Flag	Indicates if a link status trap is sent. By default, the flag is enabled.
Multiple Users Flag	Indicates if a trap is sent when the same user ID is logged into the switch more than once at the same time (either through Telnet or the serial port). By default, the flag is enabled.
Spanning Tree Flag	Indicates if a spanning tree trap is sent. By default, the flag is enabled.
ACL Traps	Indicates if an ACL trap is sent. By default, the flag is disabled.
PIM Traps	Indicates if a PIM trap is sent. By default, the flag is disabled.
Captive Portal Flag	Indicates if a captive portal trap is sent. By default, the flag is disabled.

Term	Definition
Power Supply Module state trap	Indicates if a power supply mode state trap is sent. By default, the flag is enabled.
Temperature trap	Indicates if a temperature trap is sent. By default, the flag is enabled.
Fan trap	Indicates if a fan trap is sent. By default, the flag is enabled.
MAC Notification trap flag	Indicates if a MAC notification trap is sent. By default, the flag is disabled.

show trapflags (M4350 series switch)

M4350

This command displays the trap conditions. The command output shows all enabled trap flags.

Note: You can configure which traps the switch must generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the SNMP agent on the switch sends the trap to all enabled trap receivers. Cold and warm start traps are always generated and cannot be disabled.

Format `show trapflags`

Mode Privileged EXEC

Term	Definition
Authentication Flag	Indicates if an authentication failure trap is sent. By default, the flag is enabled.
Link Up/Down Flag	Indicates if a link status trap is sent. By default, the flag is enabled.
Multiple Users Flag	Indicates if a trap is sent when the same user ID is logged into the switch more than once at the same time (either through Telnet or the serial port). By default, the flag is enabled.
Spanning Tree Flag	Indicates if a spanning tree trap is sent. By default, the flag is enabled.
ACL Traps	Indicates if an ACL trap is sent. By default, the flag is disabled.
DVMRP Traps	Indicates if a DVMRP trap is sent. By default, the flag is disabled.
OSPFv2 Traps	Indicates if an OSPFv2 trap is sent. By default, the flag is disabled. If any of the OSPFv2 trap flags are disabled, the command displays "disabled." Otherwise, the command shows the information for all enabled OSPFv2 traps.
PIM Traps	Indicates if a PIM trap is sent. By default, the flag is disabled.
OSPFv3 Traps	Indicates if an OSPFv3 trap is sent. By default, the flag is disabled. If any of the OSPFv3 trap flags are disabled, the command displays "disabled." Otherwise, the command shows the information for all enabled OSPFv3 traps.

Term	Definition
Captive Portal Flag	Indicates if a captive portal trap is sent. By default, the flag is disabled.
Power Supply Module state trap	Indicates if a power supply mode state trap is sent. By default, the flag is enabled.
Temperature trap	Indicates if a temperature trap is sent. By default, the flag is enabled.
Fan trap	Indicates if a fan trap is sent. By default, the flag is enabled.
VRRP Traps	Indicates if a VRRP trap is sent. By default, the flag is enabled.
MAC Notification trap flag	Indicates if a MAC notification trap is sent. By default, the flag is disabled.

RADIUS Commands

This section describes the commands you use to configure the switch to use a Remote Authentication Dial-In User Service (RADIUS) server on your network for authentication and accounting.

The first time that you log in as an admin user, no password is required (that is, the password is blank). After you log in for the first time, you are required to specify a new password that you must use each subsequent time that you log in. After you specify the new password, you are logged out and then must log in again, using your new password.

If you are using a RADIUS or TACAS+ server for authentication, after changing the default password to the new password, make sure that you also change the password in the RADIUS or TACAS+ server so that you can continue to log in to the switch.

aaa server radius dynamic-author

M4250

M4350

This command enables Change of Authorization (CoA) functionality and lets you configure the switch from the dynamic authorization local server configuration mode.

Format	aaa server radius dynamic-author
Mode	Global Config

no aaa server radius dynamic-author

This command disables Change of Authorization (CoA) functionality.

Format	no aaa server radius dynamic-author
Mode	Global Config

auth-type

M4250**M4350**

This command specifies the type of authorization that the switch uses for RADIUS clients. The client must match the configured attributes for authorization.

Default	all
Format	auth-type {all any session-key}
Mode	Dynamic Authorization
Term	Definition
all	Selects all COA client authentication types. All authentication attributes must match for the authentication to succeed.
any	Selects any COA client authentication type. Any authentication attribute may match for the authentication to succeed.
session-key	Indicates that the session-key must match for authentication to succeed.

no auth-type

Use this command to reset the type of authorization that the switch uses for RADIUS clients.

Format	no auth-type
Mode	Dynamic Authorization

authorization network radius

M4250**M4350**

Use this command to enable the switch to accept VLAN assignments from the RADIUS server.

Default	disable
Format	authorization network radius
Mode	Global Config

no authorization network radius

Use this command to prevent the switch from accepting VLAN assignments from the RADIUS server.

Format	no authorization network radius

Mode	Global Config

authentication command bounce-port ignore

M4250

M4350

This command configures the switch to ignore a RADIUS server **bounce-host-port** command. The **bounce-host-port** command causes a host to flap the link on an authentication port. The link flap causes DHCP renegotiation from one or more hosts connected to this port.

Default	disable (bounce-port messages are processed)

Format	authentication command bounce-port ignore

Mode	Global Config

no authentication command bounce-port ignore

This command resets the switch to the default value so that RADIUS server **bounce-host-port** commands are processed.

Format	no authentication command bounce-port ignore

Mode	Global Config

authentication command disable-port ignore

M4250

M4350

This command configures the switch to ignore a RADIUS server **disable-host-port** command. The **disable-host-port** command places the host port in the D-Disabled state with as reason CoA disabled. The port in the D-Disabled is reenabled if autorecovery is enabled for CoA and occurs after the expiration of the autorecovery timer, or you can manually reenable the port.

Default	disable (disable-port messages are processed)

Format	authentication command disable-port ignore

Mode	Global Config

no authentication command disable-port ignore

This command resets the switch to the default value so that RADIUS server **disable-host-port** commands are processed.

Format	no authentication command disable-port ignore

Mode	Global Config

clear radius dynamic-author statistics

M4250

M4350

Use this command to clear the counters for RADIUS dynamic authorization.

Format	clear radius dynamic-author statistics

Mode	Privileged EXEC

client

M4250

M4350

Use this command to configure the IP address or host name of the dynamic authorization client. Use the optional **server-key** keyword and *key-string* argument to configure the server key at the client level.

Format	client {ip-address hostname} [server-key [0 7] <i>key-string</i>]

Mode	Dynamic Authorization

no client

Use this command to remove the configured dynamic authorization client and the key that is associated with that client in the device.

Format	no client {ip-address hostname}

Mode	Dynamic Authorization

debug aaa coa

Use this command to display debug information for the dynamic authorization server process.

Format	debug aaa coa

Mode	Privileged EXEC

debug aaa pod

Use this command to display disconnect message packets.

Format	debug aaa pod

Mode	Privileged EXEC

ignore server-key

M4250

M4350

Use this command to configure the switch to ignore the server key.

Format	ignore server-key

Mode	Dynamic Authorization

no ignore server-key

Use this command to configure the switch not to ignore the server key. That is, this command resets the ignore server key property on the switch.

Format	no ignore server-key

Mode	Dynamic Authorization

ignore session-key

M4250

M4350

Use this command to configure the switch to ignore the session key.

Format	ignore session-key

Mode	Dynamic Authorization

no ignore session-key

Use this command to configure the switch not to ignore the session key. That is, this command resets the ignore session key property on the switch.

Format	no ignore session-key

Mode	Dynamic Authorization

port

M4250

M4350

Use this command to specify the UDP port on which the switch can detect RADIUS requests from the configured dynamic authorization clients. The supported range for the port number is 1025–65535.

Default	3799
Format	port <i>port-number</i>
Mode	Dynamic Authorization

no port

Use this command to reset the configured UDP port on which the switch can detect RADIUS requests from dynamic authorization clients to port number 3799, which is the default port.

Default	3799
Format	no port
Mode	Dynamic Authorization

server-key

M4250

M4350

Use this command to configure a global shared secret that is used for all dynamic authorization clients on which no individual shared secret key is configured.

Format	server-key [0 7] <i>key-string</i>
Mode	Dynamic Authorization

Parameter	Description
0	The value that you enter for the <i>key-string</i> parameter specifies an unencrypted key.
7	The value that you enter for the <i>key-string</i> parameter specifies an encrypted key.
key-string	The shared secret string. For unencrypted key, the maximum length is 128 characters.

no server-key

Use this command to remove the global shared secret key configuration.

Format	no server-key
Mode	Dynamic Authorization

radius accounting mode

M4250

M4350

This command is used to enable the RADIUS accounting function.

Default	disabled
Format	radius accounting mode
Mode	Global Config

no radius accounting mode

This command is used to set the RADIUS accounting function to the default value - i.e. the RADIUS accounting function is disabled.

Format	no radius accounting mode
Mode	Global Config

radius server attribute 4

M4250

M4350

This command specifies the RADIUS client to use the NAS-IP Address attribute in the RADIUS requests. If the specified IP address (for the server) is configured while enabling this attribute, the RADIUS client uses that IP address while sending the NAS-IP-Address attribute in RADIUS communication.

Format	radius server attribute 4 <i>ipaddr</i>
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config) #radius server attribute 4 192.168.37.60
```

no radius server attribute 4

This command disables the NAS-IP-Address attribute global parameter for a RADIUS client so that the client does not send the NAS-IP-Address attribute in RADIUS requests.

Format	no radius server attribute 4

Mode	Global Config

radius server attribute 95

M4250

M4350

This command specifies the RADIUS client to use the NAS-IPv6 Address attribute in the RADIUS requests. If the specified IPv6 address (for the server) is configured while enabling this attribute, the RADIUS client uses that IPv6 address while sending the NAS-IP-Address attribute in RADIUS communication.

Format	radius server attribute 95 <i>ipv6-address</i>

Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config) #radius server attribute 95 24::5:6
```

no radius server attribute 95

This command disables the NAS-IPv6-Address attribute global parameter for a RADIUS client so that the client does not send the NAS-IPv6-Address attribute in RADIUS requests.

Format	no radius server attribute 95

Mode	Global Config

radius server attribute 30

M4250

M4350

This command configures the format in which the MAC address is sent to the RADIUS server in attribute 30 (Called-Station-Id).

Default	legacy lower-case
Format	radius server attribute 30 mac-format {ietf legacy unformatted} {lower-case upper-case}
Mode	Global Config

Parameter	Definition
ietf	Formats the MAC address as xx-xx-xx-xx-xx-xx.
legacy	Formats the MAC address as xx:xx:xx:xx:xx:xx
unformatted	Formats the MAC address as aaaabbbbcccc.
lower-case	Formats the MAC address with lower-case characters.
upper-case	Formats the MAC address with upper-case characters.

Command example:

```
(NETGEAR Switch) (Config) #radius server attribute 30 mac-format unformatted lower-case
```

no radius server attribute 30

This command resets the format in which the MAC address is sent.

Format	no radius server attribute 30 mac-format
Mode	Global Config

radius server attribute 31

M4250**M4350**

This command configures the format in which the MAC address is sent to the RADIUS server in attribute 31 (Calling-Station-ID).

Default	legacy lower-case
Format	radius server attribute 31 mac-format {ietf legacy unformatted} {lower-case upper-case}
Mode	Global Config
Parameter	Definition
ietf	Formats the MAC address as xx-xx-xx-xx-xx-xx.
legacy	Formats the MAC address as xx:xx:xx:xx:xx:xx
unformatted	Formats the MAC address as aaaabbbbcccc.
lower-case	Formats the MAC address with lower-case characters.
upper-case	Formats the MAC address with upper-case characters.

Command example:

```
(NETGEAR Switch) (Config) #radius server attribute 31 mac-format legacy upper-case
```

no radius server attribute 31

This command resets the format in which the MAC address is sent.

Format	no radius server attribute 31 mac-format
Mode	Global Config

radius server attribute 32

M4250**M4350**

This command configures either the inclusion of and the type of NAS identifier string that is sent in attribute 32 (NAS-Identifier) or the format in which the MAC address is sent to the RADIUS server in attribute 32.

Default	For mac-format: legacy lower-case
Format	<code>radius server attribute 32 {include-in-access-req [format attribute 32 format] mac-format {ietf legacy unformatted} {lower-case upper-case}}</code>
Mode	Global Config

Parameter	Definition
<code>format attribute 32 format</code>	Enter one of the following for this argument: • Name of 2 to 128 characters • MAC address • IPV4 address • Host name • Domain name
<code>ietf</code>	Formats the MAC address as xx-xx-xx-xx-xx-xx.
<code>legacy</code>	Formats the MAC address as xx:xx:xx:xx:xx:xx
<code>unformatted</code>	Formats the MAC address as aaaabbbbcccc.
<code>lower-case</code>	Formats the MAC address with lower-case characters.
<code>upper-case</code>	Formats the MAC address with upper-case characters.

Command example:

```
(NETGEAR Switch) (Config) #radius server attribute 32 mac-format unformatted upper-case
```

`no radius server attribute 32`

This command either excludes the NAS identifier string so that it is not sent in attribute 32 or resets the format in which the MAC address is sent in attribute 32.

Format	<code>no radius server attribute 32 {include-in-access-req mac-format}</code>
Mode	Global Config

radius server attribute 44

M4250**M4350**

This command configures the inclusion of attribute 44 (Acct-Session-Id) in a RADIUS server access request.

Default	Disabled
Format	radius server attribute 44 include-in-access-req
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config) #radius server attribute 44 include-in-access-req
```

no radius server attribute 44

This command excludes attribute 44 (Acct-Session-Id) in a RADIUS server access request.

Format	no radius server attribute 44 include-in-access-req
Mode	Global Config

radius server host {ipaddr | ipv6address | hostname}

M4250**M4350**

This command configures the IPv4 address, IPv6 address, or DNS host name that must be used for communication with the RADIUS server of a selected server type. When you configure the IPv4 address, IPv6 address, or DNS host name for the authenticating or accounting servers, you can also configure the port number and server name, as well many other optional parameters (see further down in this section).

If the authenticating and accounting servers are configured without a name, the command uses the Default_RADIUS_Auth_Server and Default_RADIUS_Acct_Server as the default names, respectively. The same name can be configured for more than one authenticating servers but the name must be unique for accounting servers. The RADIUS client allows the configuration of a maximum 32 authenticating and accounting servers:

- **Authentication server:** If you use the **auth** parameter, the command configures the IPv4 address, IPv6 address, or host name that must be used to connect to a RADIUS authentication server. You can configure up to three authentication servers per RADIUS client. If the maximum number of configured servers is reached, the command fails until you remove one of the servers by issuing the **no** form of the command.
- **Accounting server:** If you use the **acct** parameter, the command configures the IPv4 address, IPv6 address, or host name that must be used for the RADIUS accounting

server. You can configure one accounting server only. If an accounting server is currently configured, use the **no** form of the command to remove it from the configuration

You can use the following optional parameters:

- **Port:** Use the optional **port** parameter to configure the UDP port number to use when connecting to the configured RADIUS server. For the **port** keyword, the *number* argument must be a value in the range 0–65535. The default UDP port number for an authentication server is 1812. The default UDP port number for an accounting server is 1813.
- **Dead time:** Use the optional **deadtime** parameter to configure the dead time that must be used for the configured RADIUS server. If the RADIUS server does not respond after the dead time (unresponsive time) period is exceeded, it is marked “dead” (unresponsive). The dead time period is from 0 to 2000 minutes. The default is 0.
- **Idle time:** Use the optional **idle-time** parameter to configure the idle time that must be used for the configured RADIUS server. If the RADIUS server does not respond after the idle time period is exceeded, the server’s state must be verified. The idle time period is from 1 to 35791 minutes. The default is 60 minutes.
- **Type:** Use the optional **type** parameter to configure the type of RADIUS server, which can be a standard server (enter **0** for the *server-type* argument) or a NETGEAR server (enter **1** for the *server-type* argument).
- **Usage:** Use the optional **usage** parameter to configure who can log in to the RADIUS server. The **login** parameter restricts authentication requests to the switch administrator. The **authmgr** parameter, restricts authentication requests to 802.1x and MAB authentications. The default **all** parameter does not restrict authentication requests.
- **Test:** Use the optional **test username** parameter to configures automated tests for configured RADIUS servers. When a test user name is configured for a RADIUS server, the client sends periodic test probes to the server. The RADIUS server responds with a reject message. The receipt of a response is an indication of liveliness of the server. Test probes are sent to the server based on the configured time interval in minutes as well as idle time.

Default	Dead time: 0 minutes Idle time: 60 minutes
Format	<code>radius server host {auth acct} {ipaddr ipv6addr dnsname} [name servername] [port number] [type server-type] [deadtime 0-2000] [idle-time 1-35791] [usage {all authmgr login}] [test username username]</code>
Mode	Global Config
Field	Description
<i>ipaddr</i>	The IPv4 address of the server.
<i>ipv6addr</i>	The IPv6 address of the server.
<i>dnsname</i>	The DNS name of the server.

Field	Description
name <i>servername</i>	The alias name to identify the server.
port <i>number</i>	The port number that is used to connect to the server. The range is from 0 to 65535.
type <i>server-type</i>	Enter one of the following options: 0. Specifies a standard server. 1. Specifies a NETGEAR server.
deadtime <i>0-2000</i>	The deadtime for the server. The range is from 0 to 2000.
idle-time <i>1-35791</i>	The idle time for the server. The range is from 1 to 35791.
usage	The usage type of the RADIUS server: - login: Restricts authentication requests to the switch administrator. - authmgr: Restricts authentication requests to 802.1x and MAB authentications. - all: Does not restrict authentication requests. This is the default setting.
test username <i>username</i>	The user name for a test configuration.

Command example:

```
(NETGEAR Switch) (Config) #radius server host acct 192.168.37.60
(NETGEAR Switch) (Config) #radius server host acct 192.168.37.60 port 1813
(NETGEAR Switch) (Config) #radius server host acct 192.168.37.60 name Network1_RS port
1813
(NETGEAR Switch) (Config) #radius server host auth 192.168.37.65 name Network2_RS
```

no radius server host

This command deletes the configured server entry from the list of configured RADIUS servers. If the RADIUS authenticating server being removed is the active server in the servers that are identified by the same server name, the RADIUS client selects another server for RADIUS transactions. If you use the **auth** parameter, the previously configured RADIUS authentication server is removed from the configuration. Similarly, if you use the **acct** parameter, the previously configured RADIUS accounting server is removed from the configuration. The *ipaddr*, *ipv6addr*, or *dnsname* argument must match the IP address or DNS name of the previously configured RADIUS authentication or accounting server.

Format	no radius server host {auth acct} {ipaddr ipv6addr dnsname} [idle-time] [usage] [test username]
Mode	Global Config

radius server host link local

M4250

M4350

This command configures the link local address and outgoing interface that must be used for communication with the RADIUS server of a selected server type. The outgoing interface can be any physical interface, service port, or network port. When you configure the link local address and outgoing interface for the authenticating or accounting servers, you can also configure the port number and server name, as well many other optional parameters (see further down in this section).

If the authenticating and accounting servers are configured without a name, the command uses the Default_RADIUS_Auth_Server and Default_RADIUS_Acct_Server as the default names, respectively. The same name can be configured for more than one authenticating servers but the name must be unique for accounting servers. The RADIUS client allows the configuration of a maximum 32 authenticating and accounting servers:

- **Authentication server:** If you use the **auth** parameter, the command configures the IPv4 address, IPv6 address, or host name that must be used to connect to a RADIUS authentication server. You can configure up to three authentication servers per RADIUS client. If the maximum number of configured servers is reached, the command fails until you remove one of the servers by issuing the **no** form of the command.
- **Accounting server:** If you use the **acct** parameter, the command configures the IPv4 address, IPv6 address, or host name that must be used for the RADIUS accounting server. You can configure one accounting server only. If an accounting server is currently configured, use the **no** form of the command to remove it from the configuration

You can use the following optional parameters:

- **Port:** Use the optional **port** parameter to configure the UDP port number to use when connecting to the configured RADIUS server. For the **port** keyword, the *number* argument must be a value in the range 0–65535. The default UDP port number for an authentication server is 1812. The default UDP port number for an accounting server is 1813.
- **Dead time:** Use the optional **deadtime** parameter to configure the dead time (unresponsive time) that must be used for the configured RADIUS server. If the RADIUS server does not respond after the dead time period is exceeded, it is marked “dead” (unresponsive). The dead time period is from 0 to 2000 minutes. The default is 0.
- **Idle time:** Use the optional **idle-time** parameter to configure the idle time that must be used for the configured RADIUS server. If the RADIUS server does not respond after the idle time period is exceeded, the server’s state must be verified. The idle time period is from 1 to 35791 minutes. The default is 60 minutes.
- **Type:** Use the optional **type** parameter to configure the type of RADIUS server, which can be a standard server (enter **0** for the *server-type* argument) or a NETGEAR server (enter **1** for the *server-type* argument).
- **Usage:** Use the optional **usage** parameter to configure who can log in to the RADIUS server. The **login** parameter restricts authentication requests to the switch administrator. The **authmgr** parameter, restricts authentication requests to 802.1x and

MAB authentications. The default **all** parameter does not restrict authentication requests.

- **Test:** Use the optional **test username** parameter to configure automated tests for configured RADIUS servers. When a test user name is configured for a RADIUS server, the client sends periodic test probes to the server. The RADIUS server responds with a reject message. The receipt of a response is an indication of liveliness of the server. Test probes are sent to the server based on the configured time interval in minutes as well as idle time.

Default	Dead time: 0 minutes Idle time: 60 minutes
Format	<code>radius server host {auth acct} {link-local <i>link-local-address</i>} {interface {unit/slot/port network serviceport} [name <i>servername</i>] [port <i>number</i>] [type <i>server-type</i>] [deadtime 0-2000] [idle-time 1-35791] [usage {all authmgr login}] [test username <i>username</i>]}</code>
Mode	Global Config
Field	Description
<code>link-local</code> <i>link-local-address</i>	The IPv4 address, IPv6 address, or host name of the local link.
<code>interface</code>	The interface that connects to the RADIUS server: • <code>unit/slot/port</code>: The interface in the unit/slot/port format. • <code>network</code>: The network interface. • <code>serviceport</code>: The service port.
<code>name <i>servername</i></code>	The alias name to identify the server.
<code>port <i>number</i></code>	The port number that is used to connect to the server. The range is from 0 to 65535.
<code>type <i>server-type</i></code>	Enter one of the following options: • 0. Specifies a standard server. • 1. Specifies a NETGEAR server.
<code>deadtime 0-2000</code>	The deadtime for the server. The range is from 0 to 2000.
<code>idle-time 1-35791</code>	The idle time for the server. The range is from 1 to 35791.
<code>usage</code>	The usage type of the RADIUS server: • <code>login</code>: Restricts authentication requests to the switch administrator. • <code>authmgr</code>: Restricts authentication requests to 802.1x and MAB authentications. • <code>all</code>: Does not restrict authentication requests. This is the default setting.
<code>test username</code> <i>username</i>	The user name for a test configuration.

Command example:

```
(NETGEAR Switch) (Config) radius server host auth link-local fe80::208:a1ff:fe7e:4519
interface network name auth_server port 1813
```

no radius server host link-local

This command deletes the configured server entry from the list of configured RADIUS servers. If the RADIUS authenticating server being removed is the active server in the servers that are identified by the same server name, the RADIUS client selects another server for RADIUS transactions. If you use the **auth** parameter, the previously configured RADIUS authentication server is removed from the configuration. Similarly, if you use the **acct** parameter, the previously configured RADIUS accounting server is removed from the configuration. The *link-local-address* argument must match the link local address of the previously configured RADIUS authentication or accounting server.

Format	no radius server host {auth acct} link-local <i>link-local-address</i>

Mode	Global Config

radius server key

M4250

M4350

This command configures the key to be used in RADIUS client communication with the specified server. Depending on whether the auth or acct token is used, the shared secret is configured for the RADIUS authentication or RADIUS accounting server. The IP address or hostname provided must match a previously configured server. When this command is executed, the secret is prompted.

Text-based configuration supports Radius server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the output of the **show running-config** command (for information about the command, see [show running-config on page 286](#)), these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Note: The secret must be an alphanumeric value not exceeding 16 characters.

Format	radius server key [{auth acct} {ipaddr ipv6address hostname}] encrypted password

Mode	Global Config

Parameter	Description
<i>ipaddr</i>	The IPv4 address of the server.
<i>ipv6address</i>	The IPv6 address of the server.

Parameter	Description
<i>hostname</i>	The host name of the server.
<i>password</i>	The password in encrypted format.

```
(NETGEAR Switch) (Config) radius server key acct 10.240.4.10 encrypted abcdef12345
```

no radius server key

This command removes the shared secret used for the RADIUS servers.

Format	no radius server key {auth acct} { <i>ipaddr</i> <i>ipv6address</i> <i>dnsname</i> }
Mode	Global Config

radius server msgauth

M4250

M4350

This command enables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

Format	radius server msgauth { <i>ipaddr</i> <i>ipv6address</i> <i>hostname</i> }
Mode	Global Config

Parameter	Description
<i>ipaddr</i>	The IPv4 address of the server.
<i>ipv6address</i>	The IPv6 address of the server.
<i>hostname</i>	The host name of the server.

no radius server msgauth

This command disables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

Format	no radius server msgauth { <i>ipaddr</i> <i>ipv6address</i> <i>hostname</i> }
Mode	Global Config

radius server primary

M4250

M4350

This command specifies a configured server that should be the primary server in the group of servers which have the same server name. Multiple primary servers can be configured for each number of servers that have the same name. When the RADIUS client has to perform transactions with an authenticating RADIUS server of specified name, the client uses the primary server that has the specified server name by default. If the RADIUS client fails to communicate with the primary server for any reason, the client uses the backup servers configured with the same server name. These backup servers are identified as the Secondary type.

Format	<code>radius server primary {ipaddr ipv6address hostname}</code>
Mode	Global Config
Field	Description
<i>ip addr</i>	The IPv4 address of the server
<i>ipv6address</i>	The IPv6 address of the server.
<i>hostname</i>	The host name of the server.

radius server retransmit

M4250

M4350

This command configures the global parameter for the RADIUS client that specifies the number of transmissions of the messages to be made before attempting the fall back server upon unsuccessful communication with the current RADIUS authenticating server. When the maximum number of retries are exhausted for the RADIUS accounting server and no response is received, the client does not communicate with any other server.

Default	4
Format	<code>radius server retransmit retries</code>
Mode	Global Config
Field	Description
<i>retries</i>	The maximum number of transmission attempts in the range of 1 to 15.

no radius server retransmit

This command sets the value of this global parameter to the default value.

Format	<code>no radius server retransmit</code>
Mode	Global Config

radius source-interface

M4250

M4350

Use this command to specify the physical or logical interface to use as the RADIUS client source interface (Source IP address). If configured, the address of source Interface is used for all RADIUS communications between the RADIUS server and the RADIUS client. The selected source-interface IP address is used for filling the IP header of RADIUS management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch.

If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address. If the configured interface is down, the RADIUS client falls back to its default behavior.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>radius source-interface {unit/slot/port loopback loopback-id vlan vlan-id serviceport}</code>
Mode	Global Config

Parameter	Description
unit/slot/port	The unit identifier assigned to the switch.
loopback-id	Configures the loopback interface. The range of the loopback ID is 0 to 7.
vlan-id	Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.
serviceport	The service port IP address is used.

no radius source-interface

Use this command to reset the RADIUS source interface to the default settings.

Format	no radius source-interface

Mode	Global Config

radius server load-balance

M4250

M4350

This command configures the load-balancing algorithm used by the RADIUS client to manage authentication and accounting requests sent to configured RADIUS servers. The load-balancing configuration is configured for a group of RADIUS servers or global default RADIUS server group. A server group is identified as a group of RADIUS servers using the same configured server name.

The supported load-balancing method is based on the least number of outstanding requests. In this mode, the RADIUS client selects a configured RADIUS server that has the least number of pending requests. Before selecting a new server, the number of pending requests on the current server in use should be more than configured batch size value.

Default	Method: None Batch size: 25

Format	radius server load-balance {auth acct} {radius name <i>servername</i> } method {none least-outstanding [<i>batch-size</i> 1-2147483647]}

Mode	Global Config

Parameter	Description
auth	Configures the RADIUS authenticating server group.
acct	Configures the RADIUS accounting server group.
radius	The RADIUS servers use the default identification name.
name <i>servername</i>	The name of the RADIUS server group.
method	This selection determines the load-balancing: • none: Load-balancing is disabled. • least-outstanding: Load-balancing is based on the lower number of outstanding request. As an option, you can use the <i>batch-size</i> argument and set the batch size to a number from 1 to 2147483647.

Command example:

```
(NETGEAR Switch) (Config) # radius server load-balance acct name group1 method
least-outstanding batch-size 40
(NETGEAR Switch) (Config) # radius server load-balance auth radius method
least-outstanding batch-size 30
```

no radius server load-balance

Use this command to disable the load-balancing algorithm used by the RADIUS client to manage authentication and accounting requests sent to configured RADIUS servers.

Format	no radius server load-balance {auth acct} {radius name <i>servername</i> } method
Mode	Global Config

radius server timeout

M4250

M4350

This command configures the global parameter for the RADIUS client that specifies the time-out value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received. The time-out value is an integer in the range of 1 to 30 seconds.

Default	5
Format	radius server timeout <i>seconds</i>
Mode	Global Config

Field	Description
retries	Maximum number of transmission attempts in the range 1–30.

no radius server timeout

This command sets the time-out global parameter to the default value.

Format	no radius server timeout
Mode	Global Config

radius server vsa send

M4250

M4350

This command enables the processing of dynamic ACL vendor-specific attributes sent by the RADIUS server. Use the **authentication** keyword to allow the processing of attributes for authentication.

Default	Disabled
Format	radius server vsa send [authentication]
Mode	Global Config

no radius server vsa send

This command disables the processing of dynamic ACL vendor-specific attributes sent by the RADIUS server.

Format	no radius server vsa send [authentication]
Mode	Global Config

radius server dead-criteria

M4250

M4350

This command configures either the time in seconds after which a RADIUS server does not respond or the number of connection attempts to which the RADIUS server does not respond. When the RADIUS server does not respond, it is marked “dead” (unresponsive). If you configure the time-out period, you can also configure the number of attempts. If the number of attempts is exceeded before the time-out period is reached, the RADIUS server is marked “dead.”

The time-out is from 1 to 120 seconds. The number of attempts is from 1 to 100.

Default	Disabled
Format	radius server dead-criteria {time 1-120 [tries 1-100] tries 1-100}
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config) # radius server dead-criteria time 40 tries 6
```

no radius server dead-criteria

This command disables the time-out period or the number of failed connection attempts to a RADIUS server so that the server is not marked “dead” if it is unresponsive.

Format	no radius server dead-criteria {time tries}
Mode	Global Config

radius server deadtime

M4250**M4350**

This command configures the “dead time” or unresponsive time (in minutes) for all RADIUS authentication servers. The dead time is the period after which a RADIUS server that is not responding to authentication requests is ignored. The dead time is from 0 to 2000 minutes. If you configure 0, the feature is disabled, that is, an unresponsive RADIUS server is not ignored.

Default	0
Format	radius server deadtime 0-2000
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config)# radius server deadtime 1800
```

no radius server deadtime

This command disables the deadtime feature so that an unresponsive RADIUS server is not ignored.

Format	no radius server deadtime
Mode	Global Config

show radius

M4250**M4350**

This command displays the values configured for the global parameters of the RADIUS client.

Format	show radius
Mode	Privileged EXEC

Term	Definition
Number of Configured Authentication Servers	The number of RADIUS Authentication servers that are configured.
Number of Configured Accounting Servers	The number of RADIUS Accounting servers that are configured.

Term	Definition
Number of Named Authentication Server Groups	The number of configured named RADIUS server groups.
Number of Named Accounting Server Groups	The number of configured named RADIUS server groups.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Time Duration	The configured timeout value, in seconds, for request retransmissions.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in the NAS-IP-Address attribute to be used in RADIUS requests.

Command example:

```
(NETGEAR Switch) #show radius
```

```

Number of Configured Authentication Servers..... 32
Number of Configured Accounting Servers..... 32
Number of Named Authentication Server Groups..... 15
Number of Named Accounting Server Groups..... 3
Number of Retransmits..... 4
Time Duration..... 10
RADIUS Accounting Mode..... Disable
RADIUS Attribute 4 Mode..... Enable
RADIUS Attribute 4 Value ..... 192.168.37.60

```

show radius servers**M4250****M4350**

This command displays the summary and details of RADIUS authenticating servers configured for the RADIUS client.

Format	<code>show radius servers [ipaddr ipv6address hostname] [name servername]</code>
Mode	Privileged EXEC

Fully Managed Switches M4250 and M4350 Series

Field	Description
<i>ipaddr</i>	The IP address of the authenticating server.
<i>ipv6address</i>	The IP address of the authenticating server.
<i>hostname</i>	The host name of the authenticating server.
name <i>servername</i>	The alias name to identify the server.
Current	The * symbol preceding the server host address specifies that the server is currently active.
Host Address	The IP address of the host.
Server Name	The name of the authenticating server.
Port	The port used for communication with the authenticating server.
Type	Specifies whether this server is a primary or secondary type.
Current Host Address	The IP address of the currently active authenticating server.
Secret Configured	Yes or No Boolean value that indicates whether this server is configured with a secret.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Message Authenticator	A global parameter to indicate whether the Message Authenticator attribute is enabled or disabled.
Time Duration	The configured timeout value, in seconds, for request retransmissions.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in NAS-IP-Address attribute used in RADIUS requests.

Command example:

```
(NETGEAR Switch) #show radius servers
```

Current	Host Address	Server Name	Port	Type
*	192.168.37.200	Network1_RADIUS_Server	1813	Primary
	192.168.37.201	Network2_RADIUS_Server	1813	Secondary
	192.168.37.202	Network3_RADIUS_Server	1813	Primary
	192.168.37.203	Network4_RADIUS_Server	1813	Secondary

Command example:

```
(NETGEAR Switch) #show radius servers name
```

Current Host Address	Server Name	Type
192.168.37.200	Network1_RADIUS_Server	Secondary
192.168.37.201	Network2_RADIUS_Server	Primary
192.168.37.202	Network3_RADIUS_Server	Secondary
192.168.37.203	Network4_RADIUS_Server	Primary

Command example:

```
(NETGEAR Switch) #show radius servers name Default_RADIUS_Server
```

```
Server Name..... Default_RADIUS_Server
Host Address..... 192.168.37.58
Secret Configured..... No
Message Authenticator ..... Enable
Number of Retransmits..... 4
Time Duration..... 10
RADIUS Accounting Mode..... Disable
RADIUS Attribute 4 Mode..... Enable
RADIUS Attribute 4 Value ..... 192.168.37.60
```

Command example:

```
(NETGEAR Switch) #show radius servers 192.168.37.58
```

```
Server Name..... Default_RADIUS_Server
Host Address..... 192.168.37.58
Secret Configured..... No
Message Authenticator ..... Enable
Number of Retransmits..... 4
Time Duration..... 10
RADIUS Accounting Mode..... Disable
RADIUS Attribute 4 Mode..... Enable
RADIUS Attribute 4 Value ..... 192.168.37.60
```

show radius accounting**M4250****M4350**

This command displays a summary of configured RADIUS accounting servers.

Format	show radius accounting name [servername]

Mode	Privileged EXEC

Fully Managed Switches M4250 and M4350 Series

Field	Description
servername	An alias name to identify the server.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.

If you do not specify any parameters, then only the accounting mode and the RADIUS accounting server details are displayed.

Term	Definition
Host Address	The IP address of the host.
Server Name	The name of the accounting server.
Port	The port used for communication with the accounting server.
Secret Configured	Yes or No Boolean value indicating whether this server is configured with a secret.

Command example:

```
(NETGEAR Switch) #show radius accounting name
```

Host Address	Server Name	Port	Secret Configured
-----	-----	-----	-----
192.168.37.200	Network1_RADIUS_Server	1813	Yes
192.168.37.201	Network2_RADIUS_Server	1813	No
192.168.37.202	Network3_RADIUS_Server	1813	Yes
192.168.37.203	Network4_RADIUS_Server	1813	No

Command example:

```
(NETGEAR Switch) #show radius accounting name Default_RADIUS_Server
```

```
Server Name..... Default_RADIUS_Server
Host Address..... 192.168.37.200
RADIUS Accounting Mode..... Disable
Port ..... 1813
Secret Configured ..... Yes
```

show radius accounting statistics

M4250**M4350**

This command displays a summary of statistics for the configured RADIUS accounting servers.

Format `show radius accounting statistics {ipaddr | ipv6address | hostname | name servername}`

Mode Privileged EXEC

Term	Definition
<i>ipaddr</i>	The IP address of the authenticating server.
<i>ipv6address</i>	The IP address of the authenticating server.
<i>hostname</i>	The host name of the authenticating server.
<i>servername</i>	The alias name to identify the server.
RADIUS Accounting Server Name	The name of the accounting server.
Server Host Address	The IP address of the host.
Round Trip Time	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.
Requests	The number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.
Retransmission	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Responses	The number of malformed RADIUS Accounting-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 as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
Timeouts	The number of accounting timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown types, which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

Command example:

```
(NETGEAR Switch) #show radius accounting statistics 192.168.37.200

RADIUS Accounting Server Name..... Default_RADIUS_Server
Host Address..... 192.168.37.200
Round Trip Time..... 0.00
Requests..... 0
Retransmissions..... 0
Responses..... 0
Malformed Responses..... 0
Bad Authenticators..... 0
Pending Requests..... 0
Timeouts..... 0
Unknown Types..... 0
Packets Dropped..... 0
```

Command example:

```
(NETGEAR Switch) #show radius accounting statistics name Default_RADIUS_Server

RADIUS Accounting Server Name..... Default_RADIUS_Server
Host Address..... 192.168.37.200
Round Trip Time..... 0.00
Requests..... 0
Retransmissions..... 0
Responses..... 0
Malformed Responses..... 0
Bad Authenticators..... 0
Pending Requests..... 0
Timeouts..... 0
Unknown Types..... 0
Packets Dropped..... 0
```

show radius source-interface**M4250****M4350**

Use this command in Privileged EXEC mode to display the configured RADIUS client source-interface (Source IP address) information.

Format	show radius source-interface

Mode	Privileged Exec

Command example:

```
(NETGEAR Switch)# show radius source-interface
RADIUS Client Source Interface..... (not configured)
```

show radius statistics

M4250

M4350

This command displays the summary statistics of configured RADIUS authenticating servers.

Format	show radius statistics { <i>ipaddr</i> <i>ipv6address</i> <i>hostname</i> name <i>servername</i> }
Mode	Privileged EXEC
Term	Definition
<i>ipaddr</i>	The IP address of the authenticating server.
<i>ipv6address</i>	The IP address of the authenticating server.
<i>hostname</i>	The host name of the authenticating server.
<i>servername</i>	The alias name to identify the server.
RADIUS Server Name	The name of the authenticating server.
Server Host Address	The IP address of the host.
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 RADIUS authentication 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 as 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 have not yet timed out or received a response.

Term	Definition
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of 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.

Command example:

```
(NETGEAR Switch) #show radius statistics 192.168.37.200
RADIUS Server Name..... Default_RADIUS_Server
Server Host Address..... 192.168.37.200
Access Requests..... 0.00
Access Retransmissions..... 0
Access Accepts..... 0
Access Rejects..... 0
Access Challenges..... 0
Malformed Access Responses..... 0
Bad Authenticators..... 0
Pending Requests..... 0
Timeouts..... 0
Unknown Types..... 0
Packets Dropped..... 0
```

Command example:

```
(NETGEAR Switch) #show radius statistics name Default_RADIUS_Server
RADIUS Server Name..... Default_RADIUS_Server
Server Host Address..... 192.168.37.200
Access Requests..... 0.00
Access Retransmissions..... 0
Access Accepts..... 0
Access Rejects..... 0
Access Challenges..... 0
Malformed Access Responses..... 0
Bad Authenticators..... 0
Pending Requests..... 0
Timeouts..... 0
Unknown Types..... 0
Packets Dropped..... 0
```

show radius server dynamic-author

M4250**M4350**

Use this command to display the dynamic authorization server settings.

Format	show radius server dynamic-author

Mode	Privileged Exec

Command example:

```
(NETGEAR Switch)#show radius server dynamic-author
```

```
AdminMode..... Disabled
Port..... 3799
Auth Type..... all
Global Secret Key..... N/A
Ignore server-key..... Disabled
Ignore session-key..... Disabled
CoA Bounce-Host-Port..... Accept
CoA Disable-Host-Port..... Accept
```

```
Client Address      Secret
-----
```

show radius server dynamic-author statistics

M4250**M4350**

Use this command to display the global counters and per-client counters of the Dynamic Authorization Server (DAS).

You can use the optional **client** keyword to narrow down the statistics for all clients or a specific client. For a specific client, specify the *ip-address*, *ipv6-address*, or *hostname* argument.

Format	show radius server dynamic-author statistics [client {all ip-address ipv6-address hostname}]

Mode	Privileged Exec

Command example:

```
(NETGEAR Switch)# show radius server dynamic-author statistics
```

```
Number of CoA Requests Received..... 5
Number of CoA ACK Responses Sent..... 2
```

Fully Managed Switches M4250 and M4350 Series

```
Number of CoA NAK Responses Sent..... 3
Number of CoA Requests Ignored..... 1
Number of CoA Missing/Unsupported Attribute R.. 0
Number of CoA Session Context Not Found Reque.. 2
Number of CoA Invalid Attribute Value Request.. 0
Number of Administratively Prohibited Request.. 0
```

Command example:

```
(NETGEAR Switch)# show radius server dynamic-author statistics client all
DAC Address..... 10.89.108.26
Number of CoA Requests Received..... 4
Number of CoA ACK Responses Sent..... 0
Number of CoA NAK Responses Sent..... 4
Number of CoA Requests Ignored..... 0
Number of CoA Missing/Unsupported Attribute Requests.. 0
Number of CoA Session Context Not Found Requests..... 4
Number of CoA Invalid Attribute Value Requests..... 0
Number of Administratively Prohibited Requests..... 0
```

```
DAC Address..... 10.52.139.190
Number of CoA Requests Received..... 3
Number of CoA ACK Responses Sent..... 0
Number of CoA NAK Responses Sent..... 3
Number of CoA Requests Ignored..... 3
Number of CoA Missing/Unsupported Attribute Requests.. 0
Number of CoA Session Context Not Found Requests..... 0
Number of CoA Invalid Attribute Value Requests..... 0
Number of Administratively Prohibited Requests..... 0
```

Command example:

```
(NETGEAR Switch)# show radius server dynamic-author statistics client 10.89.108.26
DAC Address..... 10.89.108.26
Number of CoA Requests Received..... 4
Number of CoA ACK Responses Sent..... 0
Number of CoA NAK Responses Sent..... 4
Number of CoA Requests Ignored..... 0
Number of CoA Missing/Unsupported Attribute Requests.. 0
Number of CoA Session Context Not Found Requests..... 4
Number of CoA Invalid Attribute Value Requests..... 0
Number of Administratively Prohibited Requests..... 0
```

TACACS+ Commands

TACACS+ provides access control for networked devices via one or more centralized servers. Similar to RADIUS, this protocol simplifies authentication by making use of a single database that can be shared by many clients on a large network. TACACS+ is based on the TACACS protocol (described in RFC1492) but additionally provides for separate authentication, authorization, and accounting services. The original protocol was UDP based with messages passed in clear text over the network; TACACS+ uses TCP to ensure reliable delivery and a shared key configured on the client and server to encrypt all messages.

The first time that you log in as an admin user, no password is required (that is, the password is blank). After you log in for the first time, you are required to specify a new password that you must use each subsequent time that you log in. After you specify the new password, you are logged out and then must log in again, using your new password.

If you are using a RADIUS or TACAS+ server for authentication, after changing the default password to the new password, make sure that you also change the password in the RADIUS or TACAS+ server so that you can continue to log in to the switch.

tacacs-server host

M4250

M4350

Use the **tacacs-server host** command in Global Configuration mode to configure a TACACS+ server. This command enters into the TACACS+ configuration mode. The *ip-address* or *hostname* argument is the IP address or host name of the TACACS+ server. To specify multiple hosts, multiple **tacacs-server host** commands can be used.

Format	<code>tacacs-server host {<i>ip-address</i> <i>ipv6address</i> <i>hostname</i>}</code>
Mode	Global Config

no tacacs-server host

Use the **no tacacs-server host** command to delete the specified hostname or IP address. The *ip-address*, *ipv6address*, or *hostname* argument is the IP4 or IP6 address or host name of the TACACS+ server.

Format	<code>no tacacs-server host {<i>ip-address</i> <i>ipv6address</i> <i>hostname</i>}</code>
Mode	Global Config

tacacs-server key

M4250**M4350**

Use the **tacacs-server key** command to set the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. The *key-string* parameter has a range of 0–128 characters and specifies the authentication and encryption key for all TACACS communications between the switch and the TACACS+ server. This key must match the key used on the TACACS+ daemon.

Text-based configuration supports TACACS server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the output of the **show running-config** command (for information about the command, see [show running-config on page 286](#)), these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Format	<code>tacacs-server key [key-string encrypted key-string]</code>
Mode	Global Config

no tacacs-server key

Use the **no tacacs-server key** command to disable the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. The *key-string* parameter has a range of 0–128 characters. This key must match the key used on the TACACS+ daemon.

Format	<code>no tacacs-server key key-string</code>
Mode	Global Config

tacacs-server keystring

M4250**M4350**

Use the **tacacs-server keystring** command to set the global authentication encryption key used for all TACACS+ communications between the TACACS+ server and the client.

Format	<code>tacacs-server keystring</code>
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config) #tacacs-server keystring
Enter tacacs key:*****Re-enter tacacs key:*****
```

tacacs-server source-interface

M4250**M4350**

Use this command in Global Configuration mode to configure the source interface (Source IP address) for TACACS+ server configuration. The selected source-interface IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch.

If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address.

Format	<code>tacacs-server source-interface {unit/slot/port loopback loopback-id serviceport vlan vlan-id}</code>
Mode	Global Config
Parameter	Description
unit/slot/port	The unit identifier assigned to the switch, in unit/slot/port format.
loopback-id	The loopback interface. The range of the loopback ID is 0 to 7.
serviceport	The service port IP address is used.
vlan-id	Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.

Command example:

```
(Config)#tacacs-server source-interface loopback 0
(Config)#tacacs-server source-interface 1/0/1
(Config)#no tacacs-server source-interface
```

no tacacs-server source-interface

Use this command in Global Configuration mode to remove the global source interface (Source IP selection) for all TACACS+ communications between the TACACS+ client and the server.

Format	<code>no tacacs-server source-interface</code>
Mode	Global Config

tacacs-server timeout

M4250**M4350**

Use the **tacacs-server timeout** command to set the time-out value in seconds for communication with the TACACS+ servers. The *seconds* argument is a number in the range

of 1–30 seconds. If you do not specify a time-out value, the command sets the global time-out to the default value. TACACS+ servers that do not use the global time-out will retain their configured time-out values.

Default	5
Format	<code>tacacs-server timeout [seconds]</code>
Mode	Global Config

`no tacacs-server timeout`

Use the **no tacacs-server timeout** command to restore the default timeout value for all TACACS servers.

Format	<code>no tacacs-server timeout</code>
Mode	Global Config

key (TACACS Config)

Use the **key** command in TACACS Configuration mode to specify the authentication and encryption key for all TACACS communications between the device and the TACACS server. This key must match the key used on the TACACS daemon. The *key-string* argument specifies the key name. For an empty string use `"`. (Range: 0 - 128 characters).

Text-based configuration supports TACACS server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the output of the **show running-config** command (for information about the command, see [show running-config](#) on page 286), these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Format	<code>key [key-string encrypted key-string]</code>
Mode	TACACS Config

keystring (TACACS Config)

M4250

M4350

Use the *keystring* command in TACACS Server Configuration mode to set the TACACS+ server-specific authentication encryption key used for all TACACS+ communications between the TACACS+ server and the client.

Format	<code>keystring</code>
Mode	TACACS Server Config

Command example:

```
(NETGEAR Switch) (Config) #tacacs-server host 1.1.1.1
(NETGEAR Switch) (Tacacs) #keystring
```

```
Enter tacacs key:*****
Re-enter tacacs key:*****
```

port (TACACS Config)**M4250****M4350**

Use the **port** command in TACACS Configuration mode to specify a server port number. The server *port-number* argument is a number in the range 0–65535.

Use the command without the *port-number* argument to return the port number to the default.

Default	49
Format	<i>port port-number</i>
Mode	TACACS Config

priority (TACACS Config)**M4250****M4350**

Use the **priority** command in TACACS Configuration mode to specify the order in which servers are used, where 0 (zero) is the highest priority. The *priority* argument specifies the priority for servers. The highest priority is 0 (zero), and the range is 0–65535.

Use the command without the *priority* argument to return the priority to the default.

Default	0
Format	<i>priority priority</i>
Mode	TACACS Config

timeout (TACACS Config)**M4250****M4350**

Use the **timeout** command in TACACS Configuration mode to specify the time-out value in seconds. The *seconds* argument is a number in the range 1–30 seconds as specifies the time-out.

Use the command without the *seconds* argument to return the time-out value to the default.

Default	5
Format	timeout <i>seconds</i>
Mode	TACACS Config

show tacacs

M4250

M4350

Use the **show tacacs** command to display the configuration and statistics of the TACACS+ client.

Format	show tacacs [<i>ip-address</i> <i>ipv6-address</i> <i>hostname</i> <i>client</i> <i>server</i>]
Mode	Privileged EXEC

Term	Definition
Host address	The IP4 or IPv6 address or host name of the configured TACACS+ server.
Port	The configured TACACS+ server port number.
TimeOut	The timeout in seconds for establishing a TCP connection.
Priority	The preference order in which TACACS+ servers are contacted. If a server connection fails, the next highest priority server is contacted.
Link Local Interface	If configured, the link local IPv6 address.

show tacacs source-interface

M4250

M4350

Use the **show tacacs source-interface** command in to display the configured global source interface details used for a TACACS+ client. The IP address of the selected interface is used as source IP for all communications with the server.

Format	show tacacs source-interface
Mode	Privileged EXEC

Command example:

```
(Config)# show tacacs source-interface
```

```
TACACS Client Source Interface      : loopback 0
TACACS Client Source IPv4 Address  : 1.1.1.1 [UP]
```

Configuration Scripting Commands

Configuration Scripting allows you to generate text-formatted script files representing the current configuration of a system. You can upload these configuration script files to a PC or UNIX system and edit them. Then, you can download the edited files to the system and apply the new configuration. You can apply configuration scripts to one or more switches with no or minor modifications.

Use the **show running-config** command (see [show running-config on page 286](#)) to capture the running configuration into a script. Use the **copy** command (see [copy on page 315](#)) to transfer the configuration script to or from the switch.

Use the **show** command to view the configuration stored in the startup-config, backup-config, or factory-defaults file (see [show startup-config | backup-config | factory-defaults on page 288](#)).

Use scripts on systems with default configurations; however, you are not prevented from applying scripts on systems with non-default configurations.

Scripts must conform to the following rules:

- For an M4350 series switch, script files are not distributed across the stack and remain only in the unit that is the primary management unit at the time of the file download.
- The file extension must be “.scr”.
- A maximum of ten scripts are allowed on the switch.
- The combined size of all script files on the switch shall not exceed 2048 KB.
- The maximum number of configuration file command lines is 2000.

You can type single-line annotations at the command prompt to use when you write test or configuration scripts to improve script readability. The exclamation point (!) character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line, and all input following this character is ignored. Any command line that begins with the “!” character is recognized as a comment line and ignored by the parser.

The following lines show an example of a script:

```
! Script file for displaying management access

show telnet !Displays the information about remote connections

! Display information about direct connections

show serial

! End of the script file!
```

To specify a blank password for a user in the configuration script, you must specify it as a space within quotes. For example, to change the password for user jane from a blank password to hello, the script entry is as follows:

```
users passwd jane
" "
hello
hello
```

script apply

M4250

M4350

This command applies the commands in the script to the switch. The *scriptname* argument is the name of the script to apply.

Format	<code>script apply <i>scriptname</i></code>
Mode	Privileged EXEC

script delete

M4250

M4350

This command deletes a specified script where the *scriptname* argument is the name of the script to delete. The **all** option deletes all the scripts present on the switch.

Format	<code>script delete {<i>scriptname</i> all}</code>
Mode	Privileged EXEC

script list

M4250

M4350

This command lists all scripts present on the switch as well as the remaining available space.

Format	<code>script list</code>
Mode	Privileged EXEC

Term	Definition
Configuration Script	Name of the script.
Size	Privileged EXEC

script show

M4250

M4350

This command displays the contents of a script file, which you specify with the *scriptname* argument.

Format	<code>script show scriptname</code>
Mode	Privileged EXEC
Term	Definition
Output Format	line number: line contents

script validate

M4250

M4350

This command validates a script file by parsing each line in the script file, in which *scriptname* is the name of the script to validate. The validate option is intended to be used as a tool for script development. Validation identifies potential problems. It might not identify all problems with a specified script on all devices.

Format	<code>script validate scriptname</code>
Mode	Privileged EXEC

script dhcpclient-config list

M4250

M4350

This command displays the DHCP client configuration files, including the file names and file sizes.

Format	<code>script dhcpclient-config list</code>
Mode	Privileged EXEC

script dhcpclient-config show

M4250

M4350

This command displays the contents of a specific DHCP client configuration file (*cfgfilename*), including the file names and file sizes.

Format	script dhcpclient-config show <i>cfgfilename</i>

Mode	Privileged EXEC

script dhcpclient-config delete

M4250

M4350

This command deletes a specific DHCP client configuration file (*cfgfilename*) or all DHCP client configuration files.

Format	script dhcpclient-config delete { <i>cfgfilename</i> all}

Mode	Privileged EXEC

Prelogin Banner, System Prompt, and Host Name Commands

This section describes the commands you use to configure the prelogin banner and the system prompt. The prelogin banner is the text that displays before you login at the `User:` prompt.

copy (pre-login banner)

M4250

M4350

The **copy** command includes the option to upload or download the CLI Banner to or from the switch. You can specify local URLs by using FTP, TFTP, SFTP, SCP, or Xmodem.

Note: The *ip6address* argument is also a valid parameter for routing packages that support IPv6.

Default	none
Format	copy <tftp://<ipaddr>/<filepath>/<filename>> nvram:clibanner copy nvram:clibanner <tftp://<ipaddr>/<filepath>/<filename>>
Mode	Privileged EXEC

set prompt

M4250

M4350

This command changes the name of the prompt. The length of name may be up to 64 alphanumeric characters.

Format	set prompt <i>prompt-string</i>
Mode	Privileged EXEC

hostname

M4250

M4350

This command sets the system host name. It also changes the prompt. The length of name may be up to 64 alphanumeric, case-sensitive characters.

Format	hostname <i>hostname</i>
Mode	Privileged EXEC

show clibanner

M4250

M4350

Use this command to display the configured prelogin CLI banner. The prelogin banner is the text that displays before displaying the CLI prompt.

Default	No contents to display before displaying the login prompt.
Format	show clibanner
Mode	Privileged Exec

Command example:

```
(NETGEAR Switch) #show clibanner
```

Banner Message configured:

=====

TEST

set clibanner

M4250

M4350

Use this command to configure the prelogin CLI banner before displaying the login prompt.

Format	<code>set clibanner line</code>
Mode	Global Config
Parameter	Description
line	Banner text where "" (double quote) is a delimiting character. The banner message can be up to 2000 characters.

no set clibanner

Use this command to unconfigure the prelogin CLI banner.

Format	<code>no set clibanner</code>
Mode	Global Config

Application Commands

Application commands enable you to manage applications that run on the switch.

application install

M4250

M4350

This command specifies how an executable file must start an application on the switch and how the application must run on the switch. You can enter the command (that is, preconfigure the command) for an executable file that is not yet present on the switch. The configuration does not take into effect until the executable file is present on the switch.

Format	<code>application install <i>filename</i> [start-on-boot] [auto-restart] [cpu-sharing <i>number</i>] [max-megabytes <i>megabytes</i>]</code>

Mode	Global Config

Parameter	Description
filename	The name of the file that contains the executable or script that is started as a Linux process for the application.
start-on-boot	Starts the application each time the switch boots. When you specify this keyword, the application start the first time that the switch boots after you saved the command.
auto-restart	Automatically restarts the application's processes if they stop running.
cpu-sharing number	Sets the CPU share allocated to this application. For the <i>number</i> argument, enter a number from 0 to 99 that represents a percentage. If you leave the default of 0, the CPU share for the application processes is not limited.
Max-megabytes megabytes	Sets the maximum memory resource that the application processes can consume. For the <i>megabytes</i> argument, enter a number from 0 to 200 that represents MB. If you leave the default of 0, the memory resources for the application processes are not limited.

no application install

This command removes the execution configuration for an application on the switch. If the application is running, all processes associated with the application are stopped automatically.

Format	<code>no application install <i>filename</i></code>

Mode	Global Config

application start

M4250

M4350

This command starts the execution of a specified application. The application must be installed on the switch before it can be started using this command.

Format	<code>application start <i>filename</i></code>

Mode	Global Config

application stop

M4250**M4350**

This command stops the execution of a specified application.

Format	<code>application stop filename</code>
Mode	Global Config

erase application

M4250**M4350**

Use this command to erase an executable application file that is stored in nonvolatile memory on the switch.

Format	<code>erase application filename</code>
Mode	Global Config

show application

M4250**M4350**

This command displays the applications that are installed on the switch and execution configurations of the applications.

Format	<code>show application</code>
Mode	Privileged EXEC

Field	Description
Name	The name of the application.
Start-On-Boot	Indicates whether the application is configured to start when the switch boots: Yes. The application starts when the switch boots. No. The application does not start when the switch boots.
Auto-Restart	Indicates whether the application is configured to restart when the application process stops: Yes. The application restarts when the application process stops. No. The application does not restart when the application process stops.
CPU Sharing	The command application CPU utilization limit expressed as a percentage. If the utilization is not limited, None is displayed.

Field	Description
Max Memory	The application memory usage limit in megabytes. If the memory usage is not limited, None is displayed.
Preload	Indicates if the application is pre-installed (pre-loaded) on the switch: • Yes. The application is pre-installed. • No. The application is not pre-installed.
Version	The version of the application.

show application files

M4250

M4350

This command displays the files in the application directory of the switch file system.

Format	show application files
Mode	Privileged EXEC

Field	Description
filename	The name of the application.
file size	The number of bytes that the file uses in the file system.
directory size	The number of bytes that all files in the application directory use.

OpenFlow Commands

Note: OpenFlow commands are supported on the M4350 series switches but not on the M4250 series switches.

The OpenFlow feature enables the switch to be managed by a centralized OpenFlow Controller using the OpenFlow protocol.

openflow enable

M4350

This command enables the OpenFlow feature.

Default	Disabled
Format	<code>openflow enable</code>
Mode	Global Config

no openflow enable

This command disables the OpenFlow feature.

Format	<code>no openflow enable</code>
Mode	Global Config

openflow static-ip

M4350

This command sets the IPv4 address that must be used for the OpenFlow feature. The static IP address is applied only when the static IP mode is enabled. The switch must have an operational IP interface with the specified address for the static IP address that must be used for the OpenFlow feature.

Default	0.0.0.0
Format	<code>openflow static-ip ip-address</code>
Mode	Global Config

no openflow enable

This command resets the IPv4 address for the OpenFlow feature to 0.0.0.0.

Format	<code>no openflow static-ip</code>
Mode	Global Config

openflow controller

M4350

This command sets an IP address to which the switch must establish an OpenFlow Controller connection. You can set twenty such IP addresses, but each command invocation can specify a maximum of five IP addresses and one type of connection mode (TCP or SSL). If you do not specify the IP port, the default IP port number (6633) is used. The default

connection mode is SSL. The controller table that you can configure with this command is used by the switch in OpenFlow 1.0 or 1.3 modes.

Default	None
Format	<code>openflow controller ip-address [ip-port] [ssl tcp]</code>
Mode	Global Config

Parameter	Description
<i>ip-address</i>	Up to five IP addresses (separated by a space) to which the switch must establish an OpenFlow Controller connection.
<i>ip-port</i>	The IP port that must be used for an OpenFlow Controller connection. If you do not specify the IP port, the default IP port number (6633) is used
ssl or tcp	The connection mode (TCP or SSL). The default is SSL.

no openflow controller

This command deletes a specific OpenFlow Controller IP address or all OpenFlow Controller IP addresses. If you delete a specific IP address and do not state the IP port number, all entries for the specified IP address are deleted.

Format	<code>no openflow controller {ip-address [ip-port] all}</code>
Mode	Global Config

openflow default-table

M4350

This command configures the hardware table that is used as the target for flows installed by an OpenFlow 1.0 Controller, which is not enhanced to handle multiple hardware tables. The **full-match** or **layer-2-match** option is applicable only when the OpenFlow variant is set to OpenFlow 1.0:

- **full-match**: Inserts the flow into the OpenFlow 1.0 match table, which can match all OpenFlow 1.0 fields.
- **layer-2-match**: Inserts the flow into the MAC Forwarding table, which can match the MAC addresses, VLANs, and ingress ports.

Default	full-match
Format	<code>openflow default-table {full-match layer-2-match}</code>
Mode	Global Config

openflow ip-mode

M4350

This command directs the OpenFlow feature to use the configured IP address.

Default	OpenFlow assigns itself an IP address
Format	<code>openflow ip-mode {auto static serviceport}</code>
Mode	Global Config

Parameter	Description
auto	The network IP address is used.
static	The static IP address is used.
serviceport	The service port IP address is used.

no openflow ip-mode

This command directs the OpenFlow feature to automatically assign itself an IP address.

Format	<code>no openflow ip-mode</code>
Mode	Global Config

openflow passive-mode

M4350

This command enables OpenFlow passive mode.

Default	Disabled
Format	<code>openflow passive-mode</code>
Mode	Global Config

no openflow passive-mode

This command disables OpenFlow passive mode.

Format	<code>no openflow passive-mode</code>
Mode	Global Config

openflow variant

M4350

This command sets the OpenFlow version (variant): OpenFlow 1.0 or OpenFlow 1.3.

Default	OpenFlow 1.3
Format	openflow variant {openflow10 openflow13}
Mode	Global Config

clear openflow ca-cert

M4350

This command clears the Certificate Authority certificates that are used for validating the OpenFlow controllers from the switch. This command automatically disables and reenables the OpenFlow feature. The new SSL certificates are reloaded from the OpenFlow controller on the first connection to the controller, or you can manually load them with a **copy** command.

Format	clear openflow ca-cert
Mode	Privileged Config

show openflow

M4350

This command displays the status and configuration information of OpenFlow.

Format	show openflow
Mode	Privileged Exec

Term	Definition
Administrative Mode	The OpenFlow administrative mode that is specified by the openflow enable command.
Administrative Status	The operational status of OpenFlow. Although OpenFlow can be administratively enabled, it could be operationally disabled.
Disable Reason	If OpenFlow is operationally disabled, the reason why OpenFlow is disabled.
IP Address	The IPv4 address that is assigned to OpenFlow. If no IP address is assigned, the status is None.
IP Mode	The IP mode that is specified by the openflow ip-mode command. The IP mode can be Auto, Static, or ServicePort IP.
Static IP Address	The static IP address that is specified by the openflow static-ip command.
OpenFlow Variant	The OpenFlow protocol variant (mode). The OpenFlow variant can be OpenFlow 1.0 or OpenFlow 1.3.

Term	Definition
Default Table	The hardware table that is used as the target for flows that are installed by an OpenFlow 1.0 controller that is not enhanced to handle multiple hardware tables.
Passive Mode	The OpenFlow passive mode that is specified by the openflow passive-mode command.

Command example:

```
(NETGEAR Switch) #show openflow
```

```
Administrative Mode..... Enable
Administrative Status..... Disabled
Disable Reason..... No-Suitable-IP-Interface
IP Address..... None
IP Mode..... Auto
Static IP Address..... 10.1.1.1
OpenFlow Variant..... OpenFlow 1.0
Default Table..... layer-2-match
Passive Mode..... Enable
```

Command example:

```
(NETGEAR Switch) #show openflow
```

```
Administrative Mode..... Enable
Administrative Status..... Enabled
Disable Reason..... None
IP Address..... 10.27.65.64
IP Mode..... Auto
Static IP Address..... 10.1.1.1
OpenFlow Variant..... OpenFlow 1.0
Passive Mode..... Enable
```

show openflow configured controller

M4350

This command displays a list of configured OpenFlow controllers. The switch communicates with these controllers only when the OpenFlow variant (mode) is 1.0 or 1.3.

Format	show openflow configured controller
Mode	Privileged Exec

Term	Definition
IP Address	The IPv4 address of the controller.
IP Port	The IPv4 port number on the switch for the controller connection.
Connection Mode	The SSL or TCP Controller Connection mode.
Role	The role of the controller: Initiator, Equal, Responder

Command example:

```
(NETGEAR Switch) #show openflow configured controller
```

```
IP Address      IP Port  Connection Mode  Role
-----
172.21.4.217   6633    SSL              Master
```

show openflow installed flows

M4350

This command displays the list of configured flows on the switch.

Format `show openflow installed flows [dest_ip ip-address | dest_ip_port 1-65535 | dest_mac macaddr | dscp 0-63 | ether_type 0-0xFFFF | ingress_port slot/port | ip_proto 0-255 | priority 1-65535 | source_ip ip-address | source_ip_port 1-65535 | source_mac macaddr | table {4 | 24 | 25 | 60} | vlan 1-4093 | vlan_prio 0-7]`

Mode	Privileged Exec

Paramater	Definition
dest_ip	The IP address of the destination.
dest_ip_port	The port number of the destination in the range 1–65535.
dest_mac	The MAC address of the destination.
dscp	The DSCP value in the range 0–63.
ether_type	The EtherType value in the range 0–0xFFFF.
ingress_port	The slot and port for the incoming traffic.
ip_proto	The IP protocol in the range 0–255.
priority	The priority of the flow. This is a value in the range 1–65535.
source_ip	The IP address of the source.
source_ip_port	The port number of the source in the range 1–65535.
source_mac	The MAC address of the source.

Paramater	Definition
table	The table number, which can be 4, 24, 25, or 60.
vlan	The VLAN in the range 1–4093.
vlan_prio	The VLAN priority in the range 0–7.

The following table describes the terms in the command output.

Term	Definition
Flow Type	The type of flow. For example, 1.0 or Layer 2 match.
Flow Table	The hardware table in which the flow is installed.
Flow Priority	The priority of the flow in relation to other flows.
Match Criteria	The match criteria that are specified by the flow.
Ingress Port	The port on which the flow is active.
Action	The action that is specified by the flow.
Idle	The time since the flow was active.
Installed in hardware	Whether the flow is installed in the hardware.

Command example:

```
(NETGEAR Switch) #show openflow installed flows
```

```
Flow 00000000 type "1DOT0"
```

```
Match criteria:
```

```
Flow table          24 : Priority          1
```

```
Ingress port        0/0
```

```
Actions:
```

```
Action:             Drop
```

```
Status:
```

```
Duration            2 : Idle                0 : installed in hardware    1
```

```
Flow 00000000 type "1DOT0"
```

```
Match criteria:
```

```
Flow table          24 : Priority          102
```

```
Ingress port        0/0 : Ether type      88CC
```

```
Actions:Status:
```

```
Duration            55 : Idle                45 : installed in hardware    1
```

Command example:

```
(NETGEAR Switch) # show openflow installed flows
```

```
Flow 000000E1 type "1DOT3"
```

Match criteria:

```
Flow table      60 : Priority          10
Ingress port    0/1 : Src MAC  00:00:02:37:38:01 : Dst MAC  00:00:18:37:22:01
VLAN            1 : VLAN prio        1 : Ether type      0x0800
IP proto        17 : Src IP    100.0.0.225 : Dst IP        192.0.0.225
Src IP port      1 : Dst IP port      1 : TOS              32(DSCP: 8)
```

Actions:

```
New Src IP      3.3.3.3 : New SrcIP Mask 255.255.255.255 : New Dst IP      4.4.4.4
New DstIP Mask 255.255.255.255 : Egress port      0/1
```

Status:

```
Duration        5 : Idle              2 : installed in hardware  1
```

```
Flow 000001F9 type "1DOT3"
```

Match criteria:

```
Flow table      60 : Priority          10
Ingress port    0/1 : Src MAC  00:00:1A:38:38:01 : Dst MAC  00:00:30:38:22:01
VLAN            1 : VLAN prio        1 : Ether type      0x0800
IP proto        17 : Src IP    100.0.1.249 : Dst IP        192.0.1.249
Src IP port      1 : Dst IP port      1 : TOS              32(DSCP: 8)
```

Actions:

```
Egress port      0/1
```

Status:

```
Duration        2 : Idle              0 : installed in hardware  1
```

show openflow installed groups**M4350**

This command displays the list of configured groups on the switch.

Format	show openflow installed groups
Mode	Privileged Exec

The following table displays the most significant fields in the command output.

Term	Definition
Group Type	The type of group. For example, "Indirect," "All," "Select," or another type of group.
Group Id	The unique ID of the group.
Reference Count	The group reference count is used only for "Indirect" groups. This count indicates how many "Select" groups are referring to the current "Indirect" group.
Duration	The time since the group was created.
Bucket Count	The number of buckets in the group.
Reference Group Id	References the "Indirect" group ID. This field is used for a "Select" group only.

Command example:

```
(NETGEAR Switch) # show openflow installed groups
```

```
Max Indirect Group Entries..... 1234
Current Indirect Group Entries in database..... 123
```

```
Max All Group Entries..... 1234
Current All Group Entries in database..... 123
```

```
Max Select Group Entries..... 1234
Current Select Group Entries in database..... 123
```

```
Group Id 12345678 type "Indirect"
=====
```

```
Ref Count          1 : Duration          8 : Bucket Count    1
```

```
Bucket Entry List:
-----
```

```
Bucket Index       25 : Output Port       1
Src MAC 00:00:00:00:00:AB : Dst MAC 00:00:00:00:00:CD
VLAN               101 : Reference Group Id    NA
```

```
Group Id 23456789 type "All"
=====
```

```
Ref Count          NA : Duration          10 : Bucket Count    2
```

```
Bucket Entry List:
-----
```

```
Bucket Index       26 : Output Port       2
Src MAC           NA : Dst MAC           NA
```

Fully Managed Switches M4250 and M4350 Series

```
VLAN                102 : Reference Group Id    NA

Bucket Index        27 : Output Port            3
Src MAC              NA : Dst MAC                NA
VLAN                103 : Reference Group Id    NA

Group Id 34567890 type "Select"
=====
Ref Count            NA : Duration              10 : Bucket Count    3

Bucket Entry List:
-----

Bucket Index        28 : Output Port            NA
Src MAC              NA : Dst MAC                NA
VLAN                NA : Reference Group Id     12345678

Bucket Index        29 : Output Port            NA
Src MAC              NA : Dst MAC                NA
VLAN                NA : Reference Group Id     12345678

Bucket Index        30 : Output Port            NA
Src MAC              NA : Dst MAC                NA
VLAN                NA : Reference Group Id     12345678
```

show openflow table-status

M4350

This command displays the supported OpenFlow tables and reports usage information for the tables.

Format show openflow table-status {openflow10 | openflow13}

Mode Privileged Exec

Term	Definition
Flow Table	The OpenFlow table identifier. The range is 0–255.
Flow Table Name	The name of the table.
Flow Table Description	The description of the table.
Maximum Size	The platform-dependent maximum size for the flow table.
Number of Entries	The total number of entries in the table, including the entries that are pending to be deleted.
Hardware Entries	The number of entries that are currently inserted into the hardware.

Term	Definition
Software-Only Entries	The number of entries that are not installed in the hardware. This number includes entries that are pending to be inserted, entries that cannot be inserted because of a missing interface, and entries that cannot be inserted because the table is full.
Waiting for Space Entries	The number of entries that are not in the hardware because the attempt to insert them failed.
Flow Insertion Count	The total number of flows that were added to the table since the switch powered up.
Flow Deletion Count	The total number of flows that were deleted from the table since the switch powered up.
Insertion Failure Count	The total number of hardware insertion attempts that were rejected because of lack of space since the switch powered up.

Command example:

```
(NETGEAR Switch) #show openflow table-status openflow10
```

```
Flow Table.....1
Flow Table Name..... Forwarding Database
Maximum Size.....64
Number of Entries.....8
Hardware Entries.....7
Software-Only Entries.....1
Waiting for Space Entries.....0
Flow Insertion Count.....1
Flow Deletion Count.....0
Insertion Failure Count.....0
Flow Table Description:
The forwarding database maps non-multicast MAC addresses and the ports on which these
addresses are located.
```

Command example:

```
(NETGEAR Switch) #show openflow table-status openflow13
```

```
Flow Table..... 60
Flow Table Name..... Openflow 1.3
Maximum Size..... 1920
Number of Entries..... 0
Hardware Entries..... 0
Software-Only Entries..... 0
Waiting for Space Entries..... 0
Flow Insertion Count..... 0
Flow Deletion Count..... 0
Insertion Failure Count..... 0
Flow Table Description..... The Openflow 1.3 table matches on the
packet layer-2 header, including DA-MAC, SA-MAC, VLAN, Vlan priority ether type; layer-3
header, including SRC-IP, DST-IP, IP protocol, IP-TOS; layer-4 header, including UDP/TCP
```

source and dest port, ICMP type, and code; SRC-IPv6, DST-IPv6, IPv6 Flow Label, ECN, ICMPv6 type and code, source L4 Port for TCP / UDP / SCTP and input port including physical port and LAG port.

Cloud Managed Commands

Cloud managed commands enable you to manage the interaction of the switch with a cloud management agent.

The switch maintains several configuration parameters for a cloud management agent. These parameters are handled like any other configuration parameters but are not used by the switch itself. The following table lists these parameters.

Table 8. Parameters for a cloud management agent

Parameter	Description	Range	Default
Mode	Overall administrative mode for cloud managed operation.	0. Disabled 1. Enabled	0
Proxy IP Address	The IPv4 or IPv6 address of a proxy server used to access the public network.	Any valid IPv4 or IPv6 host address. Address family: 0. None 1. INET 2. INET6 An IP address of 0.0.0.0 with an address family type of None implies that this parameter is not set.	0.0.0.0 0
Proxy IP Port Number	The TCP/UDP port number that is used with the IP Address to access the proxy server.	1–65535 The value 0 is used to designate this parameter is not currently set.	0
Proxy Username	A user name for logging into the proxy server.	An ASCII string from 1 to 64 characters. The empty string "" is used to specify that this parameter is not set.	""
Proxy Password Encrypt Type	The type of encryption that is used to store user passwords securely.	0. None 1. AES 2. MD5 (not used) A password is stored and retrieved only in its encrypted form. The switch supports AES encryption only. An encryption type of None is used to specify that this parameter is not set.	0

Table 8. Parameters for a cloud management agent (continued)

Parameter	Description	Range	Default
Proxy Password	The password for the designated user name.	An ASCII string from 1 to 64 characters in plain text (that is, unencrypted) format. Alternatively, the user can supply an AES-encrypted password string of exactly 128 ASCII characters. The empty string "" is used to specify that this parameter is not set.	""
Server URL	A URL string that identifies network access to a specific cloud server.	An ASCII string from 1 to 150 characters that contains the information that is described by the agent provider. Note: The content of this string is not checked by the switch. An agent performs its own URL string validation. The empty string "" is used to specify that this parameter is not set.	""

cloud-managed

M4250**M4350**

Use this command to let the CLI enter Cloud Managed configuration mode, which lets you change the cloud managed parameters.

Format	cloud managed
Mode	Global Config

enable

M4250**M4350**

This command administratively enables a cloud management agent to perform its intended operation, including initiating network requests to the agent's cloud server.

Note: Entering the **cloud-managed** command to enable Cloud Managed Config mode does not activate a cloud management agent, which must be independently installed and started as a process on the switch. A running agent periodically checks if this mode is enabled before it communicates with its cloud server.

Format	enable
Mode	Cloud Managed Config

no enable

This command administratively disables a cloud management agent.

If a cloud management agent is administratively disabled, it continues to run in a quiet state in which no network communication or parameter changes are allowed.

Format	no enable
Mode	Cloud Managed Config

proxy-ip-address

M4250

M4350

This command defines the parameters that let a cloud management agent communicate through a proxy server that is used to access a public network.

Some private or corporate networks restrict access to a public network by forcing all traffic through a designated gateway device (also referred to as a proxy server), which is identified by its IP address and usually by a specific TCP or UDP port number. In addition, access to the proxy server might require valid login credentials in the form of a user name and password.

The command syntax allows you to enter a password as either an ASCII string in plain text of up to 64 characters or as an AES-encrypted ASCII string of precisely 128 characters.

Note: The switch stores this password internally as AES-encrypted and does not display it unencrypted in plain text format.

Format	proxy-ip-address { <i>ipv4-address</i> <i>ipv6-address</i> } [port <i>port-number</i>] [username <i>username</i>] [password [0 7] <i>password</i>]
Mode	Cloud Managed Config

Parameter	Description
<i>ipv4-address</i> <i>ipv6-address</i>	The IP address of the proxy server, which can be in either IPv4 or IPv6 format.
port <i>port number</i>	The TCP or UDP port number that is used to access the proxy server. Valid values are from 1 to 65535. The default value is 0, which specifies that this configuration value is not set.
username <i>username</i>	The proxy server login user name that must be from 1 to 64 characters in length.

Parameter	Description
[0 7]	This option let you specify the type of password: • 0. unencrypted • 7. AES-encrypted If you do not specify this option, an AES-encrypted password is assumed.
<i>password</i>	The password that must be entered together with the user name to log in to the proxy server. If you enter an encrypted password, it must already be encrypted using AES. The allowed password length depends on the type of password: • unencrypted. 1 to 64 characters • encrypted. 128 characters

no proxy-ip-address

This command removes the proxy server configuration parameters from the switch and restores the default values (see [Table 8 on page 243](#)).

Format	no proxy-ip-address
Mode	Cloud Managed Config

url

M4250

M4350

This command defines a URL string that is used by a cloud management agent to contact its cloud server in the public network. The format of the URL string is agent-specific. The string can be from 1 to 150 characters.

Note: The switch does not validate the contents of the specified URL string. The cloud management agent process might perform its own validity checking of the URL string.

Format	url
Mode	Cloud Managed Config

no url

This command removes the cloud management server URL string from the switch.

Format	no url
Mode	Cloud Managed Config

show cloud-managed

M4250**M4350**

This command displays the cloud managed configuration parameters. A parameter that is not configured is displayed as a series of dashes (-----).

Format	show cloud-managed
Mode	User EXEC Privileged EXEC
Field	Description
Administrative Mode	Indicates whether the cloud managed operation is enabled or disabled. The default is disabled.
Proxy IP Address	The IPv4 or IPv6 address of the proxy server that is used to access the public network.
Proxy IP Port Number	The TCP or UDP port number of the proxy server that is used to access the public network.
Proxy User Name	The user name that provides access to the proxy server.
Proxy Password Encryption	Indicates AES if the password is encrypted. (This is the password that provides access to the proxy server.) The actual password (encrypted or unencrypted) is not displayed.
Server URL	The URL that the cloud management agent uses to contact its cloud server. This is a free-formatted string that is agent-specific.

Command example:

The following example shows Cloud Managed mode enabled, a proxy server configured, and no cloud server URL specified.

```
(NETGEAR Switch) #show cloud-managed
```

```
Administrative Mode ..... Enabled
Proxy IP Address ..... 192.168.10.5
Proxy IP Port Number ..... 1647
Proxy User Name ..... bob
Proxy Password Encryption ..... AES
Server URL ..... -----
```

6

Utility Commands

This chapter describes the utility commands.

The chapter includes the following sections:

- [AutoInstall Commands](#)
- [CLI Output Filtering Commands](#)
- [Dual Image Commands](#)
- [System Information and Statistics Commands](#)
- [Logging Commands](#)
- [Email Alerting and Mail Server Commands](#)
- [Firmware and File Management Commands](#)
- [System Utility and Clear Commands](#)
- [Network Time Protocol Commands](#)
- [Time Zone Commands](#)
- [DHCP Server Commands](#)
- [DNS Client Commands](#)
- [IP Address Conflict Commands](#)
- [Serviceability Packet Tracing Commands](#)
- [Cable Test Command](#)
- [Power Management Commands](#)
- [USB commands](#)
- [sFlow Commands](#)
- [Switch Database Management Template Commands](#)
- [Green Ethernet Commands](#)
- [Remote Monitoring Commands](#)
- [Statistics Application Commands](#)

The commands in this chapter are in one of four functional groups:

- **Show commands.** Display switch settings, statistics, and other information.
- **Configuration commands.** Configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- **Copy commands.** Transfer or save configuration and informational files to and from the switch.
- **Clear commands.** Clear some or all of the settings to factory defaults.

AutoInstall Commands

The AutoInstall feature enables the automatic update of the image and configuration of the switch. This feature enables touchless or low-touch provisioning to simplify switch configuration and imaging.

AutoInstall includes the following support:

- Downloading an image from TFTP server using DHCP option 125. The image update can result in a downgrade or upgrade of the firmware on the switch.
- Automatically downloading a configuration file from a TFTP server when the switch is booted with no saved configuration file.
- Automatically downloading an image from a TFTP server in the following situations:
 - When the switch is booted with no saved configuration found.
 - When the switch is booted with a saved configuration that has AutoInstall enabled.

When the switch boots and no configuration file is found, it attempts to obtain an IP address from a network DHCP server. The response from the DHCP server includes the IP address of the TFTP server where the image and configuration files are located.

After acquiring an IP address and the additional relevant information from the DHCP server, the switch downloads the image file or configuration file from the TFTP server. A downloaded image is automatically installed. A downloaded configuration file is saved to non-volatile memory.

Note: AutoInstall from a TFTP server can run on any IP interface, including the network port, service port, and in-band routing interfaces (if supported). To support AutoInstall, the DHCP client is enabled operationally on the service port, if it exists, or the network port, if there is no service port.

boot autoinstall

M4250**M4350**

Use this command to operationally start or stop the AutoInstall process on the switch. The command is non-persistent and is not saved in the startup or running configuration file.

Default	stop
Format	boot autoinstall {start stop}
Mode	Privileged EXEC

boot host retrycount

M4250**M4350**

Use this command to set the number of attempts to download a configuration file from the TFTP server. The *number* argument is a number in the range 1–3.

Default	3
Format	boot host retrycount <i>number</i>
Mode	Privileged EXEC

no boot host retrycount

Use this command to set the number of attempts to download a configuration file to the default value.

Format	no boot host retrycount
Mode	Privileged EXEC

boot host dhcp

M4250**M4350**

Use this command to enable AutoInstall on the switch for the next reboot cycle. The command does not change the current behavior of AutoInstall and saves the command to NVRAM.

Default	enabled
Format	boot host dhcp
Mode	Privileged EXEC

no boot host dhcp

Use this command to disable AutoInstall for the next reboot cycle.

Format	no boot host dhcp

Mode	Privileged EXEC

boot host autosave

M4250

M4350

Use this command to automatically save the downloaded configuration file to the `startup-config` file on the switch. When autosave is disabled, you must explicitly save the downloaded configuration to non-volatile memory by using the **write memory** or **copy system:running-config nvram:startup-config** command. If the switch reboots and the downloaded configuration has not been saved, the AutoInstall process begins, if the feature is enabled.

Default	disabled

Format	boot host autosave

Mode	Privileged EXEC

no boot host autosave

Use this command to disable automatically saving the downloaded configuration on the switch.

Format	no boot host autosave

Mode	Privileged EXEC

boot host autoreboot

M4250

M4350

Use this command to allow the switch to automatically reboot after successfully downloading an image. When auto reboot is enabled, no administrative action is required to activate the image and reload the switch.

Default	enabled

Format	boot host autoreboot

Mode	Privileged EXEC

no boot host autoreboot

Use this command to prevent the switch from automatically rebooting after the image is downloaded by using the AutoInstall feature.

Format	no boot host autoreboot

Mode	Privileged EXEC

erase startup-config

M4250

M4350

Use this command to erase the text-based configuration file stored in non-volatile memory. If the switch boots and no startup-config file is found, the AutoInstall process automatically begins.

Format	erase startup-config

Mode	Privileged EXEC

erase factory-defaults

M4250

M4350

This command erases the text-based factory default file that is stored in non-volatile memory.

Format	erase factory-defaults

Mode	Privileged EXEC

erase stack-config

M4350

This command erases the stacking configuration file. This configuration file cannot be erased using the clear config command.

Format	erase stack-config

Mode	Privileged EXEC

show autoinstall

M4250

M4350

This command displays the current status of the AutoInstall process.

Format	show autoinstall
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show autoinstall
```

```
AutoInstall Mode..... Stopped
AutoInstall Persistent Mode..... Disabled
AutoSave Mode..... Disabled
AutoReboot Mode..... Enabled
AutoInstall Retry Count..... 3
```

CLI Output Filtering Commands

show "command" | include "string"

M4250

M4350

The command **show** *command* (that is, you must enter a keyword of an existing show command for the *command* parameter) is executed and the output is filtered to display only lines containing the *string* match. All other non-matching lines in the output are suppressed.

Command example:

```
(NETGEAR Switch) #show running-config | include "spanning-tree"
```

```
spanning-tree configuration name "00-02-BC-42-F9-33"
spanning-tree bpduguard
spanning-tree bpdufilter default
```

show "command" | include "string" exclude "string2"

M4250

M4350

The command **show** *command* (that is, you must enter a keyword of an existing show command for the *command* parameter) is executed and the output is filtered to only show lines containing the *string* match and not containing the *string2* match. All other non-matching lines in the output are suppressed. If a line of output contains both the include and exclude strings then the line is not displayed.

Command example:

```
(NETGEAR Switch) #show running-config | include "spanning-tree" exclude "configuration"
```

```
spanning-tree bpduguard
spanning-tree bpdufilter default
```

show "command" | exclude "string"

M4250

M4350

The command **show** *command* (that is, you must enter a keyword of an existing show command for the *command* parameter) is executed and the output is filtered to show all lines not containing the *string* match. Output lines containing the *string* match are suppressed.

Command example:

```
(NETGEAR Switch) #show interface 0/1
```

```
Packets Received Without Error..... 0
Packets Received With Error..... 0
Broadcast Packets Received..... 0
Receive Packets Discarded..... 0
Packets Transmitted Without Errors..... 0
Transmit Packets Discarded..... 0
Transmit Packet Errors..... 0
Collision Frames..... 0
Time Since Counters Last Cleared..... 281 day 4 hr 9 min 0 sec
```

Command example:

```
(NETGEAR Switch) #show interface 0/1 | exclude "Packets"
```

```
Transmit Packet Errors..... 0
Collision Frames..... 0
Time Since Counters Last Cleared..... 20 day 21 hr 30 min 9 sec
```

show "command" | begin "string"

M4250

M4350

The command **show** *command* (that is, you must enter a keyword of an existing show command for the *command* parameter) is executed and the output is filtered to show all lines beginning with and following the first line containing the *string* match. All prior lines are suppressed.

Command example:

```
(NETGEAR Switch) #show port all | begin "1/1"
```

1/1	Enable	Down	Disable	N/A	N/A
1/2	Enable	Down	Disable	N/A	N/A
1/3	Enable	Down	Disable	N/A	N/A
1/4	Enable	Down	Disable	N/A	N/A
1/5	Enable	Down	Disable	N/A	N/A
1/6	Enable	Down	Disable	N/A	N/A

show "command" | section "string"

M4250

M4350

The command **show** *command* (that is, you must enter a keyword of an existing show command for the *command* parameter) is executed and the output is filtered to show only lines included within the section(s) identified by lines containing the *string* match and ending with the first line containing the default end-of-section identifier (that is, *exit*).

Command example:

```
(NETGEAR Switch) #show running-config | section "interface 0/1"
```

```
interface 0/1
no spanning-tree port mode
exit
```

show "command" | section "string" "string2"

M4250

M4350

The command **show** *command* (that is, you must enter a keyword of an existing show command for the *command* parameter) is executed and the output is filtered to only show lines included within the section(s) identified by lines containing the *string* match and ending with the first line containing the *string2* match. If multiple sessions matching the specified string match criteria are part of the base output, then all instances are displayed.

show "command" | section "string" include "string2"

M4250

M4350

The command **show** *command* (that is, you must enter a keyword of an existing show command for the *command* parameter) is executed and the output is filtered to only show lines included within the section(s) identified by lines containing the *string* match and ending with the first line containing the default end-of-section identifier (that is, *exit*) and that include the *string2* match. This type of filter command could also include "exclude" or user-defined end-of-section identifier parameters as well.

Dual Image Commands

The switch supports a dual image feature that allows the switch to have two software images in the permanent storage. You can specify which image is the active image to be loaded in subsequent reboots. This feature allows reduced down-time when you upgrade or downgrade the software.

delete

M4250 (without the optional *unit* parameter)

M4350

This command deletes the image1 or image 2 file from the permanent storage.

On an M4350 series switch, the optional *unit* parameter is valid only for a stack member. The *unit* parameter identifies the member on which you must execute this command. When you do not enter this parameter, the command is executed on all members in the stack.

The optional all keyword deletes all core dump files or all root CA certificates.

Format	delete [<i>unit</i>] {core-dump-file [<i>all</i>] image1 image2 root-ca-certificate [<i>all</i>]}
Mode	Privileged EXEC

boot system

M4250 (without the optional *unit* parameter)

M4350

This command activates the specified image. It will be the active-image for subsequent reboots and will be loaded by the boot loader. The current active-image is marked as the backup-image for subsequent reboots. If the specified image does not exist on the system, this command returns an error message.

On an M4350 series switch, the optional *unit* parameter identifies the stack member on which you must execute this command. When you do not enter this parameter, the command is executed on all members in the stack.

Format	<code>boot system [unit] {image1 image2}</code>

Mode	Privileged EXEC

show bootvar

M4250 (without the optional *unit* parameter)

M4350

This command displays the version information and the activation status for the current images. The command also displays any text description associated with an image. This command, when used on a standalone system, displays the switch activation status.

On an M4350 series switch, the optional *unit* parameter identifies the stack member for which the image details are displayed. If you do not specify a unit number, the command displays image details for all members in the stack.

Format	<code>show bootvar [unit]</code>

Mode	Privileged EXEC

filedescr

M4250

M4350

This command associates a specified text description with an image and replaces any existing description. The command is executed on all units in a stack.

Format	<code>filedescr {image1 image2} text-description</code>

Mode	Privileged EXEC

update bootcode

M4250

M4350

This command updates the bootcode (boot loader) on the switch. The bootcode is read from the active image for subsequent reboots. The *unit* parameter identifies the member on which this command must be executed. When this parameter is not supplied, the command is executed on all units in a stack.

Format	<code>update bootcode [unit]</code>

Mode	Privileged EXEC

System Information and Statistics Commands

This section describes the commands you use to view information about system features, components, and configurations.

show arp switch (System Information and Statistics commands)

M4250

M4350

This command displays the contents of the Address Resolution Protocol (ARP) table that is associated with the IP address of the switch. This IP address learns only ARP entries that are associated with the management interfaces (network or service ports). ARP entries that are associated with routing interfaces are not listed.

Format	show arp switch
Mode	Privileged EXEC
Term	Definition
IP Address	IP address of the management interface or another device on the management network.
MAC Address	Hardware MAC address of that device.
Interface	For a service port the output is <i>Management</i> . For a network port, the output is the unit/slot/port of the physical interface.

show eventlog

M4250

M4350

This command displays the event log, which contains error messages from the system. The event log is not cleared on a system reset. The *unit* is the switch identifier.

Format	show eventlog [<i>unit</i>]
Mode	Privileged EXEC
Term	Definition
File	The file in which the event originated.
Line	The line number of the event.
Task Id	The task ID of the event.

Term	Definition
Code	The event code.
Time	The time this event occurred.
Unit	The unit for the event.

Note: Event log information is retained across a switch reset.

show hardware

M4250

M4350

This command displays inventory information for the switch.

Note: The **show version** command and the **show hardware** command display the same information. In future releases of the software, the **show hardware** command will not be available. For a description of the command output, see the command [show version on page 260](#).

Format	show hardware
Mode	Privileged EXEC

show environment

M4250

M4350

This command displays information about the temperature and status of the power supplies and fans in the system chassis.

Format	show environment
Mode	Privileged EXEC

Command example:

```
(Netgear Switch) #show environment
Fan Control Mode..... Quiet
Temp (C)..... 23
Temperature traps range: 0 to 90 degrees (Celsius)

Temperature Sensors:
```

Fully Managed Switches M4250 and M4350 Series

Unit	Sensor	Description	Temp (C)	State	Max_Temp (C)
1	1	sensor-1	23	Normal	53

Fans:

Unit	Fan	Description	Type	Speed	Duty level	State
1	1	FAN-1	Fixed	2500	25%	Operational
1	2	FAN-2	Fixed	2500	25%	Operational

Power Modules:

Unit	Power supply	Description	Type	State
1	1	PS-1	Fixed	Operational

show version

This command displays inventory information for the switch.

M4250

M4350

Note: The **show version** command replaces the **show hardware** command in future releases of the software.

Format	show version
Mode	Privileged EXEC
Term	Definition
System Description	Text used to identify the product name of this switch.
Machine Model	The machine model as defined by the Vital Product Data
Serial Number	The unique serial number for this switch.
Burned in MAC Address	The universally assigned network address.
Software Version	The release version number of the code running on the switch.
Boot Code Version	The version of the boot code software running on the switch.
CPLD Version	The version of the CPLD firmware running on the switch.

Term	Definition
Supported Java Plugin Version	The software version of the Java plugin running on the switch.
Current Time	The current time on the running on the switch.

show platform vpd

M4250

M4350

This command displays vital product data for the switch.

Format	show platform vpd
Mode	User Privileged

The following information is displayed.

Term	Definition
Operational Code Image File Name	Build Signature loaded into the switch
Software Version	Release Version Maintenance Level and Build (RVMB) information of the switch.
Timestamp	Timestamp at which the image is built

Command example:

```
(NETGEAR Switch) #show platform vpd
```

```
Operational Code Image File Name.....
NETGEAR-Ent-esw-xgs4-gto-BL20R-CS-6AIQHSr3v7m14b35
Software Version..... 3.7.14.35
Timestamp..... Thu Mar 7 14:36:14 IST 2013
```

show interface

M4250

M4350

This command displays a summary of statistics for a specific interface or a count of all CPU traffic based upon the argument.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Fully Managed Switches M4250 and M4350 Series

Format `show interface {unit/slot/port | switchport}`

Mode Privileged EXEC

The display parameters, when the argument is *unit/slot/port*, are as follows.

Field	Definition
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
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 packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffered space.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been 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.
Transmit Packets Errors	The number of outbound packets that could not be transmitted because of errors.
Collisions Frames	The best estimate of the total number of collisions on this Ethernet segment.
Number of link down events	The number of down events for the link since the switch restarted.
Load Interval	The period in seconds for which data is used to compute the load statistics. You must enter a that is a multiple of 30. The allowable range is from 30 to 600 seconds.
Received Rate (Mbps)	The approximate number of bits per second received. This value is an exponentially-weighted average and is affected by the configured load interval.
Transmitted Rate (Mbps)	The approximate number of bits per second transmitted. This value is an exponentially-weighted average and is affected by the configured load interval.
Received Error Rate	The approximate number of error bits per second received. This value is an exponentially-weighted average and is affected by the configured load interval.
Transmitted Error Rate	The approximate number of error bits per second transmitted. This value is an exponentially-weighted average and is affected by the configured load interval.
Packets Per Second Received	The approximate number of packets per second received. This value is an exponentially-weighted average and is affected by the configured load interval.

Field	Definition
Packets Per Second Transmitted	The approximate number of packets per second transmitted. This value is an exponentially-weighted average and is affected by the configured load interval.
Link Flaps	The number of up and down events for the link since the switch restarted.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

The display parameters, when the argument is **switchport** are as follows.

Term	Definition
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

show interface lag

Use this command to display configuration information about the specified LAG interface.

Format `show interface lag lag-intf-num`

Mode Privileged EXEC

Field	Definition
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received on the LAG interface
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 packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Field	Definition
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Packets Transmitted Without Error	The total number of packets transmitted out of the LAG.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been 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.
Transmit Packets Errors	The number of outbound packets that could not be transmitted because of errors.
Collisions Frames	The best estimate of the total number of collisions on this Ethernet segment.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this LAG were last cleared.

show interface ethernet

M4250

M4350

This command displays detailed statistics for a specific interface, for a LAG, for the switch port, or for all traffic.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show interface ethernet {unit/slot/port lag lag-intf-num switchport all}</code>
Mode	Privileged EXEC

If you specify a specific interface, the command displays the following information.

Term	Definition
Packets Received	Total Packets Received (Octets) - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value Utilization which is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent. Packets Received 64 Octets - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). Packets Received 65–127 Octets - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). Packets Received 128–255 Octets - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). Packets Received 256–511 Octets - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). Packets Received 512–1023 Octets - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). Packets Received 1024–1518 Octets - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). Packets Received > 1518 Octets - The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. Packets RX and TX 64 Octets - The total number of packets (including bad packets) received and 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 and 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 and 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 and 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 and 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 and 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 received and transmitted that were between 1519 and 2047 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. Packets RX and TX 1523–2047 Octets - The total number of packets received and transmitted that were between 1523 and 2047 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed.

Term	Definition
Packets Received (continued)	Packets RX and TX 2048–4095 Octets - The total number of packets received that were between 2048 and 4095 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. Packets RX and TX 4096–9216 Octets - The total number of packets received that were between 4096 and 9216 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed.
Packets Received Successfully	Total Packets Received Without Error - 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. Note that this number does not include packets directed to the broadcast address. Broadcast Packets Received - The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Packets Received with MAC Errors	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 non-integral number of octets (Alignment Error). Note that this definition of jabber is different than 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/Undersize Received - The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets). Alignment Errors - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets. FCS Errors - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets. Overruns - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.
Received Packets Not Forwarded	Total Received Packets Not Forwarded - A count of valid frames received which were discarded (in other words, 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.

Term	Definition
Packets Transmitted Octets	Total Packets Transmitted (Octets) - 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 should be sampled before and after a common interval. ----- Packets Transmitted 64 Octets - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). Packets Transmitted 65-127 Octets - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). Packets Transmitted 128-255 Octets - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). Packets Transmitted 256-511 Octets - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). Packets Transmitted 512-1023 Octets - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). Packets Transmitted 1024-1518 Octets - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). Packets Transmitted > 1518 Octets - The total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. Max Frame Size - The maximum size of the Info (non-MAC) field that this port will receive or transmit.
Packets Transmitted Successfully	Total Packets Transmitted Successfully- The number of frames that have been 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.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been 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.
Transmit Errors	Total Transmit Errors - The sum of Single, Multiple, and Excessive Collisions. FCS Errors - The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets. Underrun Errors - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.

Term	Definition
Transmit Discards	Total Transmit Packets Discards - 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 Collisions - A count of frames for which transmission on a particular interface fails due to excessive collisions. Port Membership Discards - The number of frames discarded on egress for this port due to egress filtering being enabled.
Protocol Statistics	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 in 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. STP BPDUs Transmitted - Spanning Tree Protocol Bridge Protocol Data Units sent. STP BPDUs Received - Spanning Tree Protocol Bridge Protocol Data Units received. RST BPDUs Transmitted - Rapid Spanning Tree Protocol Bridge Protocol Data Units sent. RSTP BPDUs Received - Rapid Spanning Tree Protocol Bridge Protocol Data Units received. MSTP BPDUs Transmitted - Multiple Spanning Tree Protocol Bridge Protocol Data Units sent. MSTP BPDUs Received - Multiple Spanning Tree Protocol Bridge Protocol Data Units received.
Dot1x Statistics	EAPOL Frames Transmitted - The number of EAPOL frames of any type that have been transmitted by this authenticator. EAPOL Start Frames Received - The number of valid EAPOL start frames that have been received 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.

If you use the **switchport** keyword, the following information displays.

Term	Definition
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received With Error	The total number of packets with errors (including broadcast packets and multicast packets) received by the processor.

Term	Definition
Packets Transmitted without Errors	The total number of packets transmitted out of the interface.
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.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Number of Port Link Down Events	The number of occurrences that a port link went down.
Link Flaps	The number of link flaps per interface.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

If you use the **all** keyword, the following information displays for all interfaces on the switch.

Term	Definition
Port	The Interface ID.
Bytes Tx	The total number of bytes transmitted by the interface.
Bytes Rx	The total number of bytes transmitted by the interface.
Packets Tx	The total number of packets transmitted by the interface.
Packets Rx	The total number of packets transmitted by the interface.

show interface ethernet switchport

M4250

M4350

This command displays the private VLAN mapping information for a specified interface.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show interface ethernet <i>unit/slot/port</i> switchport</code>
Mode	Privileged EXEC

The command displays the following information.

Term	Definition
Private-vlan host-association	The VLAN association for the private-VLAN host ports.
Private-vlan mapping	The VLAN mapping for the private-VLAN promiscuous ports.

show fiber-ports optics

M4250

M4350

This command displays the diagnostics information of the SFP like Temp, Voltage, Current, Input Power, Output Power, Tx Fault, and LOS. The values are derived from the SFP's A2 (Diagnostics) table using the I²C interface.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show fiber-ports optics {all unit/slot/port}
Mode	Privileged EXEC

Field	Description
Temp	Internally measured transceiver temperature.
Voltage	Internally measured supply voltage.
Current	Measured TX bias current.
Output Power	Measured optical output power relative to 1mW.
Input Power	Measured optical power received relative to 1mW.
TX Fault	Transmitter fault.
LOS	Loss of signal.

Command example:

```
(NETGEAR Switch) #show fiber-ports optics all
```

Port	Temp	Voltage	Current	Output Power	Input Power	TX	LOS
	[C]	[Volt]	[mA]	[dBm]	[dBm]	Fault	
-----	----	-----	-----	-----	-----	-----	----
0/49	39.3	3.256	5.0	-2.234	-2.465	No	No

0/50	33.9	3.260	5.3	-2.374	-40.000	No	Yes
0/51	32.2	3.256	5.6	-2.300	-2.897	No	No

show interfaces status

M4250

M4350

Use this command to display interface information, including the description, port state, speed and autonegotiation capabilities. The command is similar to the **show port all** command but displays additional fields such as the interface description and port-capability.

The interfaces displayed by the **show interfaces status** command can be physical interfaces, LAG interfaces, or VLAN routing interfaces. You can also use the **all** keyword to display all information about all types of interfaces, or the **err-disable** keyword to display information about error-disabled interfaces.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show interfaces status {all unit/slot/port vlan vlan-id lag lag-int-num err-disabled}

Mode	Privileged EXEC

Field	Description
Port	The interface that is associated with the displayed information.
Name	The descriptive user-configured name for the interface.
Link State	Indicates whether the link is up or down.
Physical Mode	The speed and duplex settings on the interface.
Physical Status	Indicates the port speed and duplex mode for physical interfaces. The physical status for LAGs is not reported. When a port is down, the physical status is unknown.
Media Type	The media type of the interface.
Flow Control	The configured 802.3x flow control mode.
VLAN	The VLAN if which the interface is a member.

show interfaces traffic

M4250**M4350**

Use this command to display traffic information for all interfaces or, as an option, for a specific interface.

Format `show interfaces traffic [unit/slot/port]`

Mode Privileged EXEC

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument `slot/port`.
- For an M4350 series switch, use the argument `unit/slot/port`, as shown in the command format.

Field	Description
Interface Name	The interface associated with the data.
Congestion Drops (Pkts)	The number of packets that were dropped on the interface because of congestion.
Tx Queue (Bytes)	The number of bytes in the transmit queue.
Rx Queue (Bytes)	The number of bytes in the receive queue.
Color Drops (Pkts) Green	The number of green packets that were dropped.
Color Drops (Pkts) Yellow	The number of yellow (conformed) packets that were dropped.
Color Drops (Pkts) Red	The number of red (exceeded) packets that were dropped.
WRED Tx Queue (KB)	The number of packets in the WRED transmit queue.
ECN Tx Queue (Pkts)	The number of packets in the ECN transmit queue.

Command example:

```
(NETGEAR Switch)#show interfaces traffic
```

Intf Name	Congestion Drops(Pkts)	Tx Queue (KB)	Rx Queue (KB)	Color Green	Drops (Pkts) Yellow	Red	WRED Tx Queue (KB)	ECN Tx (Pkts)
0/1	0	0	0	NA	0	0	0	0
0/2	0	0	0	NA	0	0	0	0
0/3	0	0	0	NA	0	0	0	0
0/4	0	0	0	NA	0	0	0	0
0/5	0	0	0	NA	0	0	0	0
0/6	0	0	0	NA	0	0	0	0
0/7	0	0	0	NA	0	0	0	0
0/8	0	0	0	NA	0	0	0	0
0/9	0	0	0	NA	0	0	0	0
0/10	0	0	0	NA	0	0	0	0
0/11	0	0	0	NA	0	0	0	0

Command example:

```
(NETGEAR Switch)#show interfaces traffic 1/0/1
```

```
Interface Name..... 1/0/1
Congestion Drops(Pkts)..... NA
Tx Queue(Bytes)..... NA
Rx Queue(Bytes)..... NA
Color Drops Green(Pkts)..... NA
Color Drops Yellow(Pkts)..... NA
Color Drops Red(Pkts)..... NA
WRED Tx Queue(KB)..... NA
ECN Tx(Pkts)..... NA
```

CoS Queue statistics

CoS	Total Drops (Pkts)	Total (KB)	Peak (KB)	Current (KB)	Average (KB)
0	NA	NA	NA	NA	NA
1	NA	NA	NA	NA	NA
2	NA	NA	NA	NA	NA
3	NA	NA	NA	NA	NA
4	NA	NA	NA	NA	NA
5	NA	NA	NA	NA	NA
6	NA	NA	NA	NA	NA

show interfaces description**M4250****M4350**

Use this command to display the description for a specific physical interface or for all physical interfaces.

The description of the interface is configurable through the existing command **description** *name*, which has a maximum length of 64 characters that is truncated to 28 characters in the output. The long form of the description can be displayed using **show port description**.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show interfaces description {unit/slot/port all}</code>

Mode	Privileged EXEC

show interfaces diag

Use this command to provide debugging information about a specific interface with a single command. The “last reason code” is printed in the output if the link is down. Use the optional **details** keyword to display multiple details about the interface.

The command consolidates all information related to port flaps, which includes the following:

- Administrative state and fault type (local or remote)
- transceiver (voltage, power, and so on)
- Software-driven disabling (such as “err-disabled” conditions)
- Statistics

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show interfaces diag <i>unit/slot/port</i> [details]
Mode	Privileged EXEC

Command example:

The following output displays when the port is up.

```
(NETGEAR Switch)#show interfaces diag 1/0/4
Thu Jan 1 00:01:09 1970
1/0/4 is Up, line protocol is up
Description :
MTU 1500 bytes, BW 1000000 kbps
LineSpeed is 1000 Full, Auto-negotiation is on
Time Since Counters Last Cleared : 0 day 0 hr 0 min 17 sec
Link Down Event Counter : 0
input rate is 0 packet/sec, 0 bits/sec
output rate is 0 packet/sec, 0 bits/sec
Input statistics:
0 packets, 0 octets
0 Multicasts, 0 Broadcasts, 0 Unicasts
0 Errors, 0 Discarded, 0 Jabber
0 Overruns, 0 FCS, 0 Undersize
Output statistics:
23 packets, 4378 octets
23 Multicasts, 0 Broadcasts, 0 Unicasts
0 Output errors, 0 Collisions, 6 Discarded
```

Command example:

The following output displays when the port is locally shut down and therefore administratively down.

```
Sun Jan 4 18:05:16 1970
0/23 is Down, line protocol status is phy-link-down
Interface is Administratively Down.
Description : abcd
MTU 1500 bytes, BW 10000000 kbps
LineSpeed is 10G Full, Auto-negotiation is off
Time Since Counters Last Cleared : 3 day 18 hr 4 min 52 sec
Link Down Event Counter : 0
input rate is 0 packet/sec, 0 bits/sec
output rate is 0 packet/sec, 0 bits/sec
Input statistics:
0 packets, 0 octets
0 Multicasts, 0 Broadcasts, 0 Unicasts
0 Errors, 0 Discarded, 0 Jabber
0 Overruns, 0 FCS, 0 Undersize
Output statistics:
23 packets, 4378 octets
23 Multicasts, 0 Broadcasts, 0 Unicasts
0 Output errors, 0 Collisions, 6 Discarded
```

Command example:

The following output displays when the port is remotely shut down and therefore administratively down.

```
0/1 is Down, line protocol status is phy-link-down
Local Fault. Reason Code - 0x0
Description :
MTU 1500 bytes, BW 100000000 kbps
LineSpeed is 100G Full, Auto-negotiation is off
Time Since Counters Last Cleared : 3 day 0 hr 48 min 25 sec
Link Down Event Counter : 0
input rate is 0 packet/sec, 0 bits/sec
output rate is 0 packet/sec, 0 bits/sec
Input statistics:
0 packets, 0 octets
0 Multicasts, 0 Broadcasts, 0 Unicasts
0 Errors, 0 Discarded, 0 Jabber
0 Overruns, 0 FCS, 0 Undersize
Output statistics:
23 packets, 4378 octets
23 Multicasts, 0 Broadcasts, 0 Unicasts
0 Output errors, 0 Collisions, 6 Discarded
```

Command example:

The following output displays when the port is down because of an “err-disabled” condition.

```
0/1 is Down, line protocol status is err-disabled
Interface down by UDLD
Description :
MTU 1500 bytes, BW 100000000 kbps
LineSpeed is 100G Full, Auto-negotiation is off
Time Since Counters Last Cleared : 3 day 0 hr 48 min 25 sec
Link Down Event Counter : 0
input rate is 0 packet/sec, 0 bits/sec
output rate is 0 packet/sec, 0 bits/sec
Input statistics:
0 packets, 0 octets
0 Multicasts, 0 Broadcasts, 0 Unicasts
0 Errors, 0 Discarded, 0 Jabber
0 Overruns, 0 FCS, 0 Undersize
Output statistics:
23 packets, 4378 octets
23 Multicasts, 0 Broadcasts, 0 Unicasts
0 Output errors, 0 Collisions, 6 Discarded
```

show fiber-ports optics-diag**M4250****M4350**

This command displays the diagnostics information of the SFP in raw data.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show fiber-ports optics-diag {all unit/slot/port}</code>
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show fiber-ports optics-diag all
Port 2/0/5
diag data =
52 00 f8 00 50 00 f9 00 89 1c 79 18 88 86 79 ae      R...P.....y...y.
96 64 08 ca 88 b8 0a be 31 2d 05 45 2b d4 05 ea      .d.....1-.E+...
3d e9 00 b6 37 2d 00 e5 00 00 00 00 00 00 00 00      =...7-.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00      .....
```



```

00 00 00 00 3f 80 00 00 00 00 00 00 01 00 00 00      ....?.....
01 00 00 00 01 00 00 00 01 00 00 00 00 00 00 50      .....P
1d 7d 80 15 2c 15 16 08 00 00 00 00 00 00 02 00      .}...,...
00 40 00 00 00 40 00 00 00 00 00 20 20 20 20 00      .@...@....
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff      .....
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff      .....
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff      .....
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff      .....
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff      .....
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff      .....
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff      .....
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff      .....

```

show fiber-ports optics-eeprom

M4250

M4350

This command displays the Electrically Erasable Programmable Read-Only Memory (EEPROM) of the SFP.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show fiber-ports optics-eeprom {unit/slot/port all}
Mode	Privileged EXEC

Command example:

```

(NETGEAR Switch) #show fiber-ports optics-eeprom 1/0/3

Port 1/0/3
vendor_name = NETGEAR
vendor_sn   = A7N2018312
date_code  = 100625
vend_pn     = AXM761
vend_rev    = 10
eeprom data = 03 04 07 10 00 00 00 00 00 00 00 03 67 00 00 00      .....g...
08 03 00 1e 4e 45 54 47 45 41 52 20 20 20 20 20      ....NETGEAR
20 20 20 20 00 00 1f 22 41 58 4d 37 36 31 20 20      ..."AXM761
20 20 20 20 20 20 20 20 31 30 20 20 03 52 00 d2      10 .R..
00 1a 00 00 41 37 4e 32 30 31 38 33 31 32 20 20      ....A7N2018312
20 20 20 20 31 30 30 36 32 35 20 20 68 f0 03 ca      100625 h...
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff      .....
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00      .....

```

```
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff .....
```

show fiber-ports optics-info

M4250

M4350

This command displays the SFP vendor related information like Vendor Name, Serial Number of the SFP, Part Number of the SFP. The values are derived from the SFP's A0 table using the I²C interface.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format show fiber-ports optics-info {all | *unit/slot/port*}

Mode Privileged EXEC

Field	Description
Vendor Name	The vendor name is a 16 character field that contains ASCII characters, left-aligned and padded on the right with ASCII spaces (20h). The vendor name shall be the full name of the corporation, a commonly accepted abbreviation of the name of the corporation, the SCSI company code for the corporation, or the stock exchange code for the corporation.
Length (50um, OM2)	This value specifies link length that is supported by the transceiver while operating in compliance with applicable standards using 50 micron multimode OM2 [500MHz*km at 850nm] fiber. A value of zero means that the transceiver does not support 50 micron multimode fiber or that the length information must be determined from the transceiver technology.
Length (62.5um, OM1)	This value specifies link length that is supported by the transceiver while operating in compliance with applicable standards using 62.5 micron multimode OM1 [200 MHz*km at 850nm, 500 MHz*km at 1310nm] fiber. A value of zero means that the transceiver does not support 62.5 micron multimode fiber or that the length information must be determined from the transceiver technology.
Vendor SN	The vendor serial number (vendor SN) is a 16 character field that contains ASCII characters, left-aligned and padded on the right with ASCII spaces (20h), defining the vendor's serial number for the transceiver. A value of all zero in the 16-byte field indicates that the vendor SN is unspecified.

Field	Description
Vendor PN	The vendor part number (vendor PN) is a 16-byte field that contains ASCII characters, left aligned and added on the right with ASCII spaces (20h), defining the vendor part number or product name. A value of all zero in the 16-byte field indicates that the vendor PN is unspecified.
BR, nominal	The nominal bit (signaling) rate (BR, nominal) is specified in units of 100 MBd, rounded off to the nearest 100 MBd. The bit rate includes those bits necessary to encode and delimit the signal as well as those bits carrying data information. A value of 0 indicates that the bit rate is not specified and must be determined from the transceiver technology. The actual information transfer rate will depend on the encoding of the data, as defined by the encoding value.
Vendor Rev	The vendor revision number (vendor rev) contains ASCII characters, left aligned and padded on the right with ASCII spaces (20h), defining the vendor's product revision number. A value of all zero in this field indicates that the vendor revision is unspecified.

Command example:

```
(NETGEAR Switch) #show fiber-ports optics-info all
```

Port	Vendor Name	Link Length		Serial Number	Part Number	Nominal Bit Rate	
		50um	62.5um			[Mbps]	Rev
		[m]	[m]				
0/49	NETGEAR	8	3	A7N2018414	AXM761	10300	10
0/51	NETGEAR	8	3	A7N2018472	AXM761	10300	10
0/52	NETGEAR	8	3	A7N2018501	AXM761	10300	10

show mac-addr-table**M4250****M4350**

This command displays the forwarding database entries. These entries are used by the transparent bridging function to determine how to forward a received frame.

Enter **a11** or no parameter to display the entire table. Enter a MAC Address and VLAN ID to display the table entry for the requested MAC address on the specified VLAN. Enter the **count** parameter to view summary information about the forwarding database table.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Use the **interface** *unit/slot/port* parameter to view MAC addresses on a specific interface. Instead of *unit/slot/port*, **lag** *lag-intf-num* can be used as an alternate

way to specify the LAG interface, in which *lag-intf-num* is the LAG port number. Use the **vlan** *vlan-id* parameter to display information about MAC addresses on a specified VLAN.

Format	<code>show mac-addr-table [macaddr vlan-id all count interface unit/slot/port vlan vlan-id]</code>
Mode	Privileged EXEC

The following information displays if you do not enter a parameter, the keyword **all**, or the MAC address and VLAN ID.

Term	Definition
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Interface	The port through which this address was learned.
Interface Index	This object indicates the ifIndex of the interface table entry associated with this port.
Status	The status of this entry. The meanings of the values are: • Static. The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be relearned. • Learned. The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use. • Management. The value of the corresponding instance (system MAC address) is also the value of an existing instance of dot1dStaticAddress. It is identified with interface 0/1. and is currently used when enabling VLANs for routing. • Self. The value of the corresponding instance is the address of one of the switch's physical interfaces (the system's own MAC address). • GMRP Learned. The value of the corresponding was learned via GMRP and applies to Multicast. • Other. The value of the corresponding instance does not fall into one of the other categories.

If you enter **vlan** *vlan-id*, only the MAC Address, Interface, and Status fields appear. If you enter the **interface** *unit/slot/port* parameter, in addition to the MAC Address and Status fields, the VLAN ID field also appears.

The following information displays if you enter the **count** parameter.

Term	Definition
Dynamic Address count	Number of MAC addresses in the forwarding database that were automatically learned.
Static Address (User-defined) count	Number of MAC addresses in the forwarding database that were manually entered by a user.

Term	Definition
Total MAC Addresses in use	Number of MAC addresses currently in the forwarding database.
Total MAC Addresses available	Number of MAC addresses the forwarding database can handle.

process cpu threshold

M4250

M4350

Use this command to configure the CPU utilization thresholds. The Rising and Falling thresholds are specified as a percentage of CPU resources. The utilization monitoring time period can be configured from 5 seconds to 86400 seconds in multiples of 5 seconds. The CPU utilization threshold configuration is saved across a switch reboot. Configuring the falling utilization threshold is optional. If the falling CPU utilization parameters are not configured, then they take the same value as the rising CPU utilization parameters.

Format	<code>process cpu threshold type total rising <i>threshold</i> interval <i>seconds</i> [falling <i>threshold</i> interval <i>seconds</i>]</code>
Mode	Global Config

Term	Description
<code>rising <i>threshold</i></code>	The percentage of CPU resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
<code>rising interval <i>seconds</i></code>	The duration of the CPU rising threshold violation, in seconds, that must be met to trigger a notification. The range is 5 to 86400. The default is 0 (disabled).
<code>falling <i>threshold</i></code>	The percentage of CPU resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled). A notification is triggered when the total CPU utilization falls below this level for a configured period of time. The falling utilization threshold notification is made only if a rising threshold notification was previously done. The falling utilization threshold must always be equal or less than the rising threshold value. The CLI does not allow setting the falling threshold to be greater than the rising threshold.
<code>falling interval <i>seconds</i></code>	The duration of the CPU falling threshold, in seconds, that must be met to trigger a notification. The range is 5 to 86400. The default is 0 (disabled).

show process app-list

M4250**M4350**

This command displays the user and system applications.

Format	show process app-list
Mode	Privileged EXEC
Field	Description
ID	The application identifier.
Name	The name that identifies the process.
PID	The number the software uses to identify the process.
Admin Status	The administrative status of the process.
Auto Restart	Indicates whether the process will automatically restart if it stops.
Running Status	Indicates whether the process is currently running or stopped.

Command example:

```
(NETGEAR Switch) #show process app-list
```

ID	Name	PID	Admin Status	Auto Restart	Running Status
1	dataplane	15309	Enabled	Disabled	Running
2	switchdrvr	15310	Enabled	Disabled	Running
3	syncdb	15314	Enabled	Disabled	Running
4	lighttpd	18718	Enabled	Enabled	Running
5	syncdb-test	0	Disabled	Disabled	Stopped
6	proctest	0	Disabled	Enabled	Stopped
7	user.start	0	Enabled	Disabled	Stopped

show process memory

M4250**M4350**

This command displays memory consumption details by various software components.

Format	show process memory
Mode	Privileged EXEC

Field	Description
Total	The total available memory on the switch.
Free	The free memory on the switch.
Allocated	The allocated memory on the switch, excluding cache space used by the file system.
Components	The internal software component.
CurrentAllocated	The amount of memory that a component is using.
Change	The increase or decrease of the memory that a component consumes since the last time this command was executed. This field shows the difference in memory allocation between two successive executions of the command.
MaxAllocated	The maximum amount of memory allocation by a component.
Allocs/Frees	The number of memory allocation and free calls made by a component.

show process cpu (M4250 series switch)

M4250

This command provides the percentage utilization of the CPU by different tasks. The optional **threshold** keyword displays CPU utilization and memory monitoring threshold information.

Note: A busy CPU might not be caused by traffic processing but by various tasks that run simultaneously.

Format `show process cpu [threshold]`

Mode Privileged EXEC

Parameter	Description
Free	The system-wide free memory.
Alloc	The system-wide allocated memory (excluding cache, file system used space).
PID	The process or thread ID.
Name	The process or thread name.
5Secs	The CPU utilization sampling in 5-second intervals.
60Secs	The CPU utilization sampling in 60-second intervals.
300Secs	The CPU utilization sampling in 300-second intervals.
Total CPU Utilization	Total CPU utilization in percentage within the specified window of 5, 60, and 300 seconds.

Command example:

```
(NETGEAR Switch) #show process cpu
```

```
Memory Utilization Report
```

```
status      bytes
```

```
-----
```

```
free       106450944
```

```
alloc      423227392
```

```
CPU Utilization:
```

PID	Name	5 Secs	60 Secs	300 Secs

765	_interrupt_thread	0.00%	0.01%	0.02%
767	bcmL2X.0	0.58%	0.35%	0.28%
768	bcmCNTR.0	0.77%	0.73%	0.72%
773	bcmRX	0.00%	0.04%	0.05%
786	cpuUtilMonitorTask	0.19%	0.23%	0.23%
834	dot1s_task	0.00%	0.01%	0.01%
810	hapiRxTask	0.00%	0.01%	0.01%
805	dtlTask	0.00%	0.02%	0.02%
863	spmTask	0.00%	0.01%	0.00%
894	ip6MapLocalDataTask	0.00%	0.01%	0.01%
908	RMONTask	0.00%	0.11%	0.12%

Total CPU Utilization		1.55%	1.58%	1.50%

show process cpu (M4350 series switch)

M4350

This command provides the percentage utilization of the CPU by different tasks. The optional **threshold** keyword displays CPU utilization and memory monitoring threshold information.

For a switch stack, the **all** keyword lets you display the process information for all members in the stack. The *number* argument can be a number from 1 to 8 and lets you display the process information for a specific stack member.

Note: A busy CPU might not be caused by traffic processing but by various tasks that run simultaneously.

Format	show process cpu [threshold all number]

Mode	Privileged EXEC

Fully Managed Switches M4250 and M4350 Series

Parameter	Description
Free	The system-wide free memory.
Alloc	The system-wide allocated memory (excluding cache, file system used space).
PID	The process or thread ID.
Name	The process or thread name.
5Secs	The CPU utilization sampling in 5-second intervals.
60Secs	The CPU utilization sampling in 60-second intervals.
300Secs	The CPU utilization sampling in 300-second intervals.
Total CPU Utilization	Total CPU utilization in percentage within the specified window of 5, 60, and 300 seconds.

Command example:

```
(NETGEAR Switch) #show process cpu
```

```
Memory Utilization Report
```

```
status      bytes
```

```
-----
```

```
free       106450944
```

```
alloc      423227392
```

```
CPU Utilization:
```

PID	Name	5 Secs	60 Secs	300 Secs
765	_interrupt_thread	0.00%	0.01%	0.02%
767	bcmL2X.0	0.58%	0.35%	0.28%
768	bcmCNTR.0	0.77%	0.73%	0.72%
773	bcmRX	0.00%	0.04%	0.05%
786	cpuUtilMonitorTask	0.19%	0.23%	0.23%
834	dot1s_task	0.00%	0.01%	0.01%
810	hapiRxTask	0.00%	0.01%	0.01%
805	dtlTask	0.00%	0.02%	0.02%
863	spmTask	0.00%	0.01%	0.00%
894	ip6MapLocalDataTask	0.00%	0.01%	0.01%
908	RMONTask	0.00%	0.11%	0.12%
Total CPU Utilization		1.55%	1.58%	1.50%

show process proc-list

M4250**M4350**

This application displays the processes started by applications created by the Process Manager.

Format	show process proc-list
Mode	Privileged EXEC
Parameter	Description
PID	The number the software uses to identify the process.
Process Name	The name that identifies the process.
Application ID-Name	The application identifier and its associated name.
Child	Indicates whether the process has spawned a child process.
VM Size	Virtual memory size.
VM Peak	The maximum amount of virtual memory the process has used.
FD Count	The file descriptors count for the process.

Command example:

```
(NETGEAR Switch) #show process proc-list
```

PID	Process Name	Application ID-Name	Chld	VM Size (KB)	VM Peak (KB)	FD Count
15260	procmgr	0-procmgr	No	1984	1984	8
15309	dataplane	1-dataplane	No	293556	293560	11
15310	switchdrvr	2-switchdrvr	No	177220	177408	57
15314	syncdb	3-syncdb	No	2060	2080	8
18718	lighttpd	4-lighttpd	No	5508	5644	11
18720	lua_magnet	4-lighttpd	Yes	12112	12112	7
18721	lua_magnet	4-lighttpd	Yes	25704	25708	7

show running-config

M4250**M4350**

Use this command to display or capture the current setting of different protocol packages supported on the switch. This command displays or captures commands with settings and

configurations that differ from the default value. To display or capture the commands with settings and configurations that are equal to the default value, include the **all** option.

Note: The **show running-config** command does not display the User Password, even if you set one different from the default.

The output is displayed in script format, which can be used to configure another switch with the same configuration. If the optional *scriptname* is provided with a file name extension of *.scr*, the output is redirected to a script file.

Note: If you issue the **show running-config** command from a serial connection, access to the switch through remote connections (such as Telnet) is suspended while the output is being generated and displayed.

Note: If you use a text-based configuration file, the **show running-config** command only displays configured physical interfaces (i.e. if any interface only contains the default configuration, that interface will be skipped from the **show running-config** command output). This is true for any configuration mode that contains nothing but default configuration. That is, the command to enter a particular config mode, followed immediately by its exit command, are both omitted from the **show running-config** command output (and hence from the *startup-config* file when the system configuration is saved.)

Use the following keys to navigate the command output.

Key	Action
Enter	Advance one line.
Space Bar	Advance one page.
q	Stop the output and return to the prompt.

Note that **--More--** or **(q)uit** is displayed at the bottom of the output screen until you reach the end of the output.

Format	<code>show running-config [all scriptname]</code>
Mode	Privileged EXEC

show running-config interface

M4250**M4350**

Use this command to display the running configuration for a specific interface. Valid interfaces include physical, LAG, loopback, and VLAN interfaces.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show running-config interface {unit/slot/port lag lag-intf-num loopback loopback-id vlan vlan-id}</code>
Mode	Privileged EXEC

Parameter	Description
slot/port or unit/slot/port	Displays the running configuration for the specified interface.
lag-intf-num	Displays the running configuration for the LAG interface.
loopback-id	Displays the running configuration for the loopback interface.
vlan-id	Displays the running configuration for the VLAN routing interface.

Command example:

```
(NETGEAR Switch) #show running-config interface 0/1
!Current Configuration:
!
interface 0/1
addport 3/1
exit
(NETGEAR Switch) #
```

show startup-config | backup-config | factory-defaults

M4250**M4350**

This command displays the content of text-based configuration files from the CLI. The text-based configuration files (startup-config, backup-config and factory-defaults) are saved

compressed in flash. With this command, the files are decompressed while displaying their content.

Format	show {startup-config backup-config factory-defaults}

Mode	Privileged EXEC

Parameter	Description
startup-config	Display the content of the startup-config file.
backup-config	Display the content of the backup-config file.
factory-defaults	Display the content of the factory-defaults file.

Command example:

```
(NETGEAR Switch) #show startup-config
```

```
!Current Configuration:
```

```
!
```

```
!System Description "NETGEAR M4350-12X12F 12x10G Copper 12x10G SFP+ Managed Switch,  
14.0.0.15, 1.0.0.4"
```

```
!System Software Version "14.0.0.15"
```

```
!System Up Time          "0 days 2 hrs 9 mins 16 secs"
```

```
!Additional Packages      QOS,Multicast,IPv6,IPv6 Management,Stacking,Routing
```

```
!Current System Time: Jun  6 22:34:10 2023
```

```
!
```

```
vlan database
```

```
vlan 20,30,40,50,60,70,80,90
```

```
vlan name 20 "Paris"
```

```
vlan name 30 "Berlin"
```

```
vlan name 40 "Amsterdam"
```

```
vlan name 50 "Brussels"
```

```
vlan name 60 "London"
```

```
vlan name 70 "Rome"
```

```
vlan name 80 "Vienna"
```

```
vlan name 90 "Stockholm"
```

```
vlan routing 1 1
```

```
exit
```

```
ip http session soft-timeout 60
```

```
configure
```

```
no sntp client mode
```

```
vlan 20
```

```
private-vlan primary
```

```
private-vlan association 30
```

```
exit
```

```
vlan 30
```

```
private-vlan isolated
```

Fully Managed Switches M4250 and M4350 Series

```
exit
vlan 40
private-vlan community
exit
username "admin" password
d71397624a65c393a945222ee6640ed7d6058002605cd2f3797f32d0d9c8c568398280e355dda0408124144
6044a37283aa2aea40bf61d4350452dc35209ce9b level 15 encrypted
line console
exit
line telnet
exit
line ssh
exit
!
snmp-server user "admin" DefaultWrite auth-md5-key c8506f0595b9bda64a94be4867c677bb
interface 0/5
switchport private-vlan mapping trunk 70 80
exit
interface 0/7
switchport mode private-vlan trunk promiscuous
exit
interface 0/8
switchport mode private-vlan trunk secondary
exit
interface vlan 1
routing
ip address dhcp
exit
router rip
exit
capture usb appie
exception protocol ftp
exception switch-chip-register enable
exception dump ftp-server 10.12.13.14 username "admin" password "Password1!"
exit
ip http secure-session soft-timeout 60
```

dir**M4250****M4350**

Use this command to list the files in flash from the CLI. For switch models that support a USB port, you can use the optional **usb** keyword to display the USB device status and details.

Format `dir [usb]`

Mode Privileged EXEC

Command example:

(NETGEAR Switch) `#dir`

```

0  drwx                2048 May 09 2002 16:47:30 .
0  drwx                2048 May 09 2002 16:45:28 ..
0  -rwx                 592 May 09 2002 14:50:24 slog2.txt
0  -rwx                 72 May 09 2002 16:45:28 boot.dim
0  -rwx                 0 May 09 2002 14:46:36 olog2.txt
0  -rwx            13376020 May 09 2002 14:49:10 image1
0  -rwx                 0 Apr 06 2001 19:58:28 fsyssize
0  -rwx            1776 May 09 2002 16:44:38 slog1.txt
0  -rwx            356 Jun 17 2001 10:43:18 crashdump.ct1
0  -rwx            1024 May 09 2002 16:45:44 sslt.rnd
0  -rwx            14328276 May 09 2002 16:01:06 image2
0  -rwx            148 May 09 2002 16:46:06 hpc_broad.cfg
0  -rwx                 0 May 09 2002 14:51:28 olog1.txt
0  -rwx            517 Jul 23 2001 17:24:00 ssh_host_key
0  -rwx            69040 Jun 17 2001 10:43:04 log_error_crashdump
0  -rwx            891 Apr 08 2000 11:14:28 sslt_key1.pem
0  -rwx            887 Jul 23 2001 17:24:00 ssh_host_rsa_key
0  -rwx            668 Jul 23 2001 17:24:34 ssh_host_dsa_key
0  -rwx            156 Apr 26 2001 13:57:46 dh512.pem
0  -rwx            245 Apr 26 2001 13:57:46 dh1024.pem
0  -rwx                 0 May 09 2002 16:45:30 slog0.txt

```

show sysinfo

M4250**M4350**

This command displays switch system information. The optional **noMibs** keyword lets you exclude MIBs information from the output.

Format	show sysinfo [noMibs]
Mode	Privileged EXEC
Field	Definition
Switch Description	Text used to identify this switch.
System Name	Name used to identify the switch. The factory default is blank. To configure the system name, see snmp-server on page 162.
System Location	Text used to identify the location of the switch. The factory default is blank. To configure the system location, see snmp-server on page 162.
System Contact	Text used to identify a contact person for this switch. The factory default is blank. To configure the system location, see snmp-server on page 162.
System ObjectID	The base object ID for the switch's enterprise MIB.
System Up Time	The time in days, hours and minutes since the last switch reboot.
Current SNTP Synchronized Time	The system time acquired from a network SNTP server.
MIBs Supported	A list of MIBs supported by this agent.

length

M4250**M4350**

Use this command to set the pagination length to value number of lines for the sessions specified by configuring on different Line Config modes (Telnet, SSH, and console). The command is persistent. The *number* argument is a number in the range of 5–48 lines. Enter 0 to specify no pagination.

Default	24 lines per page
Format	length <i>number</i>
Mode	Line Config

no length

Use this command to set the pagination length to the default value number of lines.

Format	no length

Mode	Line Config

terminal length

M4350

Use this command to set the terminal pagination length to a particular number of lines for the current session. The *number* argument is a number in the range of 5–48 lines. This command configuration takes effect immediately on the current session and is nonpersistent.

Default	24 lines per page

Format	terminal length <i>number</i>

Mode	Privileged EXEC

no terminal length

Use this command to set the terminal length to the default value number of lines.

Format	no terminal length

Mode	Privileged EXEC

show terminal length

M4250

M4350

Use this command to display all the configured terminal length values.

Format	show terminal length

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show terminal length
```

```
Terminal Length:
```

```
-----
```

```
For Current Session.....24
```

```
For Serial Console..... 24
```

```
For Telnet Sessions.....24
```

```
For SSH Sessions..... 24
```

memory free low-watermark processor

M4250

M4350

Use this command to get notifications when the CPU free memory falls below the configured threshold. A notification is generated when the free memory falls below the threshold. Another notification is generated once the available free memory rises to 10 percent above the specified threshold. To prevent generation of excessive notifications when the CPU free memory fluctuates around the configured threshold, only one Rising or Falling memory notification is generated over a period of 60 seconds. The threshold is specified in kilobytes. The CPU free memory threshold configuration is saved across a switch reboot.

Format	<code>memory free low-watermark processor <i>threshold</i></code>
Mode	Global Config
Parameter	Description
threshold	When CPU free memory falls below this threshold, a notification message is triggered. The range is 1–1017416 (the maximum available memory on the switch). The default is 0 (disabled).

mac-address-table notification change

M4250

M4350

This command enables the MAC notification feature and its parameters **history-size** and **interval**. MAC address notification lets you receive an SNMP trap or informational message when a MAC address is learned by the switch or the MAC address ages out of the MAC address table. MAC movement is treated as deletion of an entry on the old port, and addition of an entry on the new port.

Default	MAC address notification is disabled by default. The default history size is 1. The default notification interval is 1 second.
Format	<code>mac-address-table notification change [<i>history-size size</i> <i>interval seconds</i>]</code>
Mode	Global Config
Parameter	Description
history-size <i>size</i>	The size of the MAC address table. The range is from 1 to 255.
interval <i>seconds</i>	The SNMP trap notification interval. The range is from 1 to 2147483647.

no mac-address-table notification change

This command disables the MAC notification feature.

Format	no mac-address-table notification change [history-size interval]

Mode	Global Config

Switch Services Commands

This section describes the switch services commands. Switch services are services that provide support for features such as temperature, power supply status, fan control, and others. Each of these services is platform dependent. (For example, some platforms may have temperature sensors, but no fan controller. Or, others may have both while others have neither.)

environment fan control mode

M4250

M4350

Use this command to set the fan mode.

Format	environment fan control mode {auto cool off quiet}

Mode	Global Config

Parameter	Definition
auto	Sets the fans to Auto mode, which, in this firmware version, is identical to quiet mode.
cool	Sets the fans to Cool mode. In Cool mode, the fans consistently function at 100 percent speed, provide maximum cooling, and produce considerable noise. Note: In Quiet mode, the switch might automatically change back and forth between Cool mode and Quiet mode until a temperature, PoE budget, or traffic load condition returns within thresholds.
off	Sets the fans to Off mode. In Off mode, the fans produce no noise. You can only manually set the fans in Off mode. Off mode is not supported on some models.

Parameter	Definition
quiet	Sets the fans to Quiet mode, which is the default mode. In Quiet mode, the following applies: - The fans support intelligent operation, which enables the switch to automatically start the operation of the fans, gradually increase the speed of the fans, and either halt PoE or block traffic if the temperature exceeds a critical level. - The fans function from 25 to 75 percent speed and can reach 100 percent speed. At 25 percent speed, the fans produce minimal noise. Fan noise increases at 50 percent speed and even more so at 75 percent speed. At 100 percent speed, the fans produce considerable noise. Note: For detailed information about temperature thresholds, PoE budgets, and traffic load conditions that affect the fans, see the hardware installation guide, which you can download by visiting netgear.com/support/download.

Note: The fan setting changes immediately. However, depending on the switch model, if the temperature detected by the temperature sensor exceeds its threshold, a PoE budget is exceeded, or a traffic load condition is exceeded, the switch automatically overrides your manual setting.

environment temprange

M4250

M4350

Use this command to set the allowed temperature range for normal operation.

Format	<code>environment temprange min temperature max temperature</code>
Mode	Global Config

Parameter	Definition
<code>min temperature</code>	Sets the minimum allowed temperature for normal operation. The range is between –100°C and 100°C. The default is 0°C.
<code>max temperature</code>	Sets the maximum allowed temperature for normal operation. The range is between –100°C and 100°C. The default is 0°C.

environment trap

M4250**M4350**

Use this command to configure environment status traps.

Format	environment trap {fan powersupply temperature}
Mode	Global Config
Parameter	Definition
fan	Enables or disables the sending of traps for fan status events. The default is enable.
powersupply	Enables or disables the sending of traps for power supply status events. The default is enable.
temperature	Enables or disables the sending of traps for temperature status events. The default is enable.

Logging Commands

This section describes the commands you use to configure system logging, and to view logs and the logging settings.

logging buffered

M4250**M4350**

This command enables logging to an in-memory log. You can specify the severity level value as either an integer from 0 to 7 or symbolically through one of the following keywords: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), or **debug** (7).

Default	disabled; notice (5) when enabled
Format	logging buffered [severitylevel]
Mode	Global Config

no logging buffered

This command disables logging to in-memory log.

Format	no logging buffered
Mode	Global Config

logging buffered wrap

M4250**M4350**

This command enables wrapping of in-memory logging when the log file reaches full capacity. Otherwise when the log file reaches full capacity, logging stops.

Default	enabled
Format	logging buffered wrap
Mode	Privileged EXEC

no logging buffered wrap

This command disables wrapping of in-memory logging and configures logging to stop when the log file capacity is full.

Format	no logging buffered wrap
Mode	Privileged EXEC

logging buffered threshold

M4250**M4350**

This command sets the percentage (from 1 to 100 percent) of log space. If logging exceeds the threshold percentage, a console log is generated, and, if configured, an alert email is generated.

The threshold configuration applies only if the **logging buffered wrap** command is disabled. The default action for the memory log is to wrap. The threshold does not apply to that default action.

Default	enabled
Format	logging buffered threshold <i>percentage-range</i>
Mode	Global Config

Parameter	Definition
<i>percentage-range</i>	Sets the percentage of log space that, if exceeded, causing logging to stop. The range is from 1 to 100 percent. The default is 80 percent.

logging cli-command

M4250**M4350**

This command enables the CLI command logging feature, which enables the switch to log all CLI commands issued on the switch.

Default	enabled
Format	logging cli-command
Mode	Global Config

no logging cli-command

This command disables the CLI command Logging feature.

Format	no logging cli-command
Mode	Global Config

logging console

M4250**M4350**

This command enables logging to the console. You can specify the *severitylevel* value as either an integer from 0 to 7 or symbolically through one of the following keywords:

emergency (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), or **debug** (7).

Default	disabled; error (3) when enabled
Format	logging console [<i>severitylevel</i>]
Mode	Global Config

no logging console

This command disables logging to the console.

Format	no logging console
Mode	Global Config

logging host

M4250**M4350**

This command configures the logging host parameters. You can configure up to eight hosts.

Default	<i>port-number</i>. 514 <i>severitylevel</i>. 2
Format	<code>logging host {hostaddress hostname} addresstype [tls {anon x509name certificate-index}] {port-number severitylevel}</code>
Mode	Global Config
Parameter	Description
hostaddress hostname	The IP address or name of the logging host.
address-type	Indicates the type of address (IPv4, IPv6, or DNS) being passed.
tls [anon x509name]	Enables TLS security for the host through either anon (which stands for anonymous) or x509name, in which you must specify a certificate number.
certificate-index	If you select x509name, use the <i>certificate-index</i> argument to specify the certificate number that must be used for authentication. The valid range is from 0 to 8. Use 0 for the default file.
port-number	A port number from 1 to 65535.
severitylevel	Specify this value as either an integer from 0 to 7, or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).

Command example:

```
(NETGEAR Switch) (Config)# logging host google.com dns 214
(NETGEAR Switch) (Config)# logging host 10.130.64.88 ipv4 214 6
(NETGEAR Switch) (Config)# logging host 2000::150 ipv6 214 7
```

logging host reconfigure

M4250**M4350**

This command enables logging host reconfiguration.

Format	<code>logging host reconfigure hostindex</code>
Mode	Global Config

Parameter	Description
hostindex	Enter the Logging Host Index for which to change the IP address.

logging host remove

M4250

M4350

This command disables logging to host. See [show logging hosts on page 305](#) for a list of host indexes.

Format	<code>logging host remove hostindex</code>
Mode	Global Config

logging protocol

M4250

M4350

This command configures the logging protocol version number as 0 or 1. RFC 3164 uses version 0 and RFC 5424 uses version 1.

Default	0
Format	<code>logging protocol {0 1}</code>
Mode	Global Config

logging syslog

M4250

M4350

This command enables syslog logging.

Format	<code>logging syslog</code>
Mode	Global Config

no logging syslog

This command disables syslog logging.

Format	<code>no logging syslog</code>
Mode	Global Config

logging syslog port

M4250**M4350**

This command enables syslog logging. The *portid* argument is an integer in the range 1–65535.

Default	disabled
Format	logging syslog port <i>portid</i>
Mode	Global Config

no logging syslog port

This command disables syslog logging.

Format	no logging syslog port
Mode	Global Config

logging syslog usb

M4250**M4350**

For switch models that support a USB port, this command configures a USB device for the storage of syslog messages.

Format	logging syslog usb <i>file-name</i>
Mode	Global Config

logging syslog source-interface

M4250**M4350**

This command configures the syslog source-interface (source IP address) for syslog server configuration. The selected source-interface IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch. If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>logging syslog source-interface {unit/slot/port {loopback loopback-id} {vlan vlan-id} serviceport}}</code>

Mode	Global Config

Parameter	Description
slot/port or unit/slot/port	The port-based routing interface.
loopback-id	The loopback interface is used as the source IP address. The range of the loopback ID is 0 to 7.
vlan-id	The VLAN interface is used as the source IP address. The range of the VLAN ID is 1 to 4093.
serviceport	The service port IP address is used as the source IP address.

Command example:

```
(config)#logging syslog source-interface loopback 0
```

Command example:

```
(config)#logging syslog source-interface 0/4/1
```

Command example:

```
(config)#logging syslog source-interface 1/0/1
```

no logging syslog source-interface

This command disables syslog logging.

Format	<code>no logging syslog</code>

Mode	Global Config

show logging

M4250

M4350

This command displays logging configuration information.

Format	<code>show logging</code>

Mode	Privileged EXEC

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Logging Client Local Port	Port on the collector/relay to which syslog messages are sent.
Logging Client USB file name	The file name that is used to write the log to the USB device.
Logging Client Source Interface	Shows the configured syslog source-interface (source IP address).
CLI Command Logging	Shows whether CLI Command logging is enabled.
Console Logging	Shows whether console logging is enabled.
Console Logging Severity Filter	The minimum severity that is logged to the console log. Messages with an equal or lower numerical severity are logged.
Buffered Logging	Shows whether buffered logging is enabled.
Buffered Logging Severity Filter	The minimum severity that is logged to the buffered log. Messages with an equal or lower numerical severity are logged.
Buffered Logging Threshold (%)	The buffer threshold value, which represents the percentage of the total log buffer. If logging exceeds this value, a console log is generated, and, if configured, an alert email is generated
Syslog Logging	Shows whether syslog logging is enabled.
Log Messages Received	Number of messages received by the log process. This includes messages that are dropped or ignored.
Log Messages Dropped	Number of messages that could not be processed due to error or lack of resources.
Log Messages Relayed	Number of messages sent to the collector/relay.

Command example:

```
(NETGEAR Switch) #show logging

Logging Client Local Port      : 514
Logging Client USB File Name  :
Logging Client Source Interface : vlan 1
Logging Client Source IPv4 Address : 169.254.100.100      [Up]
CLI Command Logging           : disabled
Logging protocol               : 0
Console Logging                : enabled
Console Logging Severity Filter : error
Buffered Logging               : enabled
Buffered Logging Severity Filter : notice
Buffered Logging Threshold (%) : 80

Syslog Logging                 : disabled
```

```
Log Messages Received      : 39856
Log Messages Dropped      : 0
Log Messages Relayed      : 0
```

show logging buffered

M4250

M4350

This command displays buffered logging (system startup and system operation logs).

Format	show logging buffered
Mode	Privileged EXEC
Term	Definition
Buffered (In-Memory) Logging	Shows whether the In-Memory log is enabled or disabled.
Buffered Logging Wrapping Behavior	The behavior of the In Memory log when faced with a log full situation.
Buffered Log Count	The count of valid entries in the buffered log.
Buffered Log Threshold (lines)	The configured threshold value expressed as the number of log lines.

show logging hosts

M4250

M4350

This command displays all configured logging hosts. Use the “|” character to display the output filter options.

Format	show logging hosts
Mode	Privileged EXEC
Term	Definition
Host Index	Used for deleting hosts.
IP Address / Hostname	IP address or hostname of the logging host.
Severity Level	The minimum severity to log to the specified address. The possible values are emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).

Term	Definition
Port	The server port number, which is the port on the local host from which syslog messages are sent.
Status	The status of SNMP (Active, Not in Service, or Not Ready).
Mode	The type of security: UDP or TLS.
Auth	The type of authentication mode: anonymous or x509name.
Cert#	The certificate number to be used for authentication. The valid range is from 0 to 8. Index 0 is used for the default file.

Command example:

```
(NETGEAR Switch) #show logging hosts
```

Index	IP Address/Hostname	Severity	Port	Status	Mode	Auth	Cert#
-----	-----	-----	-----	-----	-----	-----	-----
1	10.130.64.88	critical	514	Active	udp		
1	2000::150	critical	514	Active	udp		

show logging traplogs**M4250****M4350**

This command displays SNMP trap events and statistics.

Format show logging traplogs

Mode Privileged EXEC

Term	Definition
Number of Traps Since Last Reset	The number of traps since the last boot.
Trap Log Capacity	The number of traps the system can retain.
Number of Traps Since Log Last Viewed	The number of new traps since the command was last executed.
Log	The log number.
System Time Up	How long the system had been running at the time the trap was sent.
Trap	The text of the trap message.

clear logging buffered

M4250

M4350

This command clears buffered logging (system startup and system operation logs).

Format	clear logging buffered

Mode	Privileged EXEC

clear eventlog

M4250

M4350

This command clears all event messages that are stored on the switch.

Format	clear eventlog

Mode	Privileged EXEC

Email Alerting and Mail Server Commands

logging email

M4250

M4350

This command enables email alerting and sets the lowest severity level for which log messages are emailed. If you specify a severity level, log messages at or above this severity level, but below the urgent severity level, are emailed in a non-urgent manner by collecting them together until the log time expires. You can specify the *severitylevel* value as either an integer from 0 to 7 or symbolically through one of the following keywords: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), or **debug** (7).

Default	disabled; when enabled, log messages at or above severity Warning (4) are emailed

Format	logging email [<i>severitylevel</i>]

Mode	Global Config

no logging email

This command disables email alerting.

Format	no logging email
Mode	Global Config

logging email urgent

M4250

M4350

This command sets the lowest severity level at which log messages are emailed immediately in a single email message. Specify the *severitylevel* value as either an integer from 0 to 7 or symbolically through one of the following keywords: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), or **debug** (7). Specify **none** to indicate that log messages are collected and sent in a batch email at a specified interval.

Default	Alert (1) and emergency (0) messages are sent immediately.
Format	logging email urgent { <i>severitylevel</i> none}
Mode	Global Config

no logging email urgent

This command resets the urgent severity level to the default value.

Format	no logging email urgent
Mode	Global Config

logging email message-type to-addr

M4250

M4350

This command configures the email address to which messages are sent. The message types supported are **urgent**, **non-urgent**, and **both**. For each supported severity level, multiple email addresses can be configured. The *to-email-addr* variable is a standard email address, for example admin@yourcompany.com.

Format	logging email message-type {urgent non-urgent both} to-addr <i>to-email-addr</i>
Mode	Global Config

no logging email message-type to-addr

This command removes the configured to-addr field of email.

Format	no logging email message-type {urgent non-urgent both} to-addr <i>to-email-addr</i>

Mode	Global Config

logging email from-addr

M4250

M4350

This command configures the email address of the sender (the switch).

Default	switch@netgear.com

Format	logging email from-addr <i>from-email-addr</i>

Mode	Global Config

no logging email from-addr

This command removes the configured email source address.

Format	no logging email from-addr <i>from-email-addr</i>

Mode	Global Config

logging email message-type subject

M4250

M4350

This command configures the subject line of the email for the specified type.

Default	For urgent messages: Urgent Log Messages For non-urgent messages: Non Urgent Log Messages

Format	logging email message-type {urgent non-urgent both} subject <i>subject</i>

Mode	Global Config

no logging email message-type subject

This command removes the configured email subject for the specified message type and restores it to the default email subject.

Format	no logging email message-type {urgent non-urgent both} subject
Mode	Global Config

logging email logtime

M4250

M4350

This command configures how frequently non-urgent email messages are sent. Non-urgent messages are collected and sent in a batch email at the specified interval. The *minutes* argument is a number in the range 30–1440 minutes.

Default	30 minutes
Format	logging email logtime <i>minutes</i>
Mode	Global Config

no logging email logtime

This command resets the non-urgent log time to the default value.

Format	no logging email logtime
Mode	Global Config

logging traps

M4250

M4350

This command sets the severity at which SNMP traps are logged and sent in an email. Specify the *severitylevel* value as either an integer from 0 to 7 or symbolically through one of the following keywords: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), or **debug** (7).

Default	Info (6) messages and higher are logged.
Format	logging traps <i>severitylevel</i>
Mode	Global Config

no logging traps

This command resets the SNMP trap logging severity level to the default value.

Format	no logging traps

Mode	Global Config

logging email test message-type

M4250

M4350

This command sends an email to the SMTP server to test the email alerting function.

Format	logging email test message-type {urgent non-urgent both} message-body <i>message-body</i>

Mode	Global Config

show logging email config

M4250

M4350

This command displays information about the email alert configuration.

Format	show logging email config

Mode	Privileged EXEC

Term	Definition
Email Alert Logging	The administrative status of the feature: enabled or disabled
Email Alert From Address	The email address of the sender (the switch).
Email Alert Urgent Severity Level	The lowest severity level that is considered urgent. Messages of this type are sent immediately.
Email Alert Non Urgent Severity Level	The lowest severity level that is considered non-urgent. Messages of this type, up to the urgent level, are collected and sent in a batch email. Log messages that are less severe are not sent in an email message at all.
Email Alert Trap Severity Level	The lowest severity level at which traps are logged.
Email Alert Notification Period	The amount of time to wait between non-urgent messages.
Email Alert To Address Table	The configured email recipients.
Email Alert Subject Table	The subject lines included in urgent (Type 1) and non-urgent (Type 2) messages.

Term	Definition
For Msg Type urgent, subject is	The configured email subject for sending urgent messages.
For Msg Type non-urgent, subject is	The configured email subject for sending non-urgent messages.

show logging email statistics

M4250

M4350

This command displays email alerting statistics.

Format	show logging email statistics
Mode	Privileged EXEC

Term	Definition
Email Alert Operation Status	The operational status of the email alerting feature.
No of Email Failures	The number of email messages that have attempted to be sent but were unsuccessful.
No of Email Sent	The number of email messages that were sent from the switch since the counter was cleared.
Time Since Last Email Sent	The amount of time that has passed since the last email was sent from the switch.

clear logging email statistics

M4250

M4350

This command resets the email alerting statistics.

Format	clear logging email statistics
Mode	Privileged EXEC

mail-server

M4250**M4350**

This command configures the SMTP server to which the switch sends email alert messages and changes the mode to Mail Server Configuration mode. The server address can be in the IPv4, IPv6, or DNS name format.

Format	<code>mail-server {ip-address ipv6-address hostname}</code>
Mode	Global Config

no mail-server

This command removes the specified SMTP server from the configuration.

Format	<code>no mail-server {ip-address ipv6-address hostname}</code>
Mode	Global Config

security (Mail Server Config)

M4250**M4350**

This command sets the email alerting security protocol by enabling the switch to use TLS authentication with the SMTP Server. If the TLS mode is enabled on the switch but the SMTP sever does not support TLS mode, no email is sent to the SMTP server.

Default	none
Format	<code>security {tlsv1 none}</code>
Mode	Mail Server Config

port (Mail Server Config)

M4250**M4350**

This command configures the TCP port to use for communication with the SMTP server. The recommended port number for TLSv1 is 465, and for no security that is, none) it is port number 25. However, any nonstandard port number in the range 1 to 65535 is also allowed.

Default	25
Format	<code>port number</code>
Mode	Mail Server Config

username (Mail Server Config)

M4250**M4350**

This command configures the login ID the switch uses to authenticate with the SMTP server.

Default	admin
Format	username <i>name</i>
Mode	Mail Server Config

password (Mail Server Config)

M4250**M4350**

This command configures the password the switch uses to authenticate with the SMTP server.

Default	admin
Format	password <i>password</i>
Mode	Mail Server Config

show mail-server config

M4250**M4350**

This command displays information about the email alert configuration.

Format	show mail-server [<i>ip-address</i> <i>hostname</i> <i>all</i>] config
Mode	Privileged EXEC

Term	Definition
No of mail servers configured	The number of SMTP servers configured on the switch.
Email Alert Mail Server Address	The IPv4/IPv6 address or DNS hostname of the configured SMTP server.
Email Alert Mail Server Port	The TCP port the switch uses to send email to the SMTP server
Email Alert Security Protocol	The security protocol (TLS or none) the switch uses to authenticate with the SMTP server.
Email Alert Username	The username the switch uses to authenticate with the SMTP server.
Email Alert Password	The password the switch uses to authenticate with the SMTP server.

Firmware and File Management Commands

This section describes the commands that you use to upload and download firmware and other files to and from the switch, and verify the digital signature of firmware and other files.

copy

M4250

M4350

The **copy** command uploads and downloads files to and from the switch. You can also use the **copy** command to update the firmware by uploading firmware (image) files and manage the dual images (image 1 and image 2) on the file system.

Upload and download files from a server using FTP, TFTP, Xmodem, Ymodem, or Zmodem. SFTP and SCP are available as additional transfer methods if the software package supports secure management. If FTP is used, a password is required.

Format	<code>copy source destination {verify noverify}</code>

Mode	Privileged EXEC

Replace the *source* and *destination* parameters with the options that are described in the table further down in this section. For the *url* source and destination arguments that are listed in the table further down in this section, use one of the following values:

- xmodem
- ymodem
- zmodem
- tftp://{ipaddress | hostname}/filepath/filename
- ftp://{user@ipaddr | hostname}/path/filename
- scp://{user@ipaddr | hostname}/path/filename
- sftp://{user@ipaddr | hostname}/path/filename
- usb://filepath/filename

The **verify** and **noverify** keywords are available only if the image/configuration verify options feature is enabled (see [file verify on page 319](#)); **verify** specifies that digital signature verification will be performed for the specified downloaded image or configuration file. **noverify** specifies that no verification will be performed.

The keyword **ias-users** supports the downloading of the IAS user database file. When the IAS users file is downloaded, the switch IAS user's database is replaced with the users and its attributes available in the downloaded file. In the command **copy url ias-users**, for *url* one of the following is used for IAS users file:

```
{{tftp://<ipaddr> | <ipv6address> | <hostname>/<filepath>/<filename>} |  
{sftp | scp://<username>@<ipaddress>/<filepath>/<filename>}}
```

Note: The maximum length for the file path is 160 characters, and the maximum length for the file name is 31 characters.

For FTP, TFTP, SFTP and SCP, the *ipaddr* or *hostname* parameter is the IP address or host name of the server, *filepath* is the path to the file, and *filename* is the name of the file you want to upload or download. For SFTP and SCP, the *username* parameter is the user name for logging into the remote server via SSH.

Note: *ipv6address* is also a valid parameter for routing packages that support IPv6.

For an M4350 series switch, to copy OpenFlow SSL certificates to the switch using TFTP or XMODEM, using only the following options pertinent to the OpenFlow SSL certificates.

Format	copy [mode/file] nvram:{openflow-ssl-ca-cert openflow-ssl-cert openflow-ssl-priv-key} [source {ip-address unit/slot/port loopback number serviceport vlan vlan-id}]
Mode	Privileged Exec



CAUTION:

Before you load a new release image to make a backup, upload the existing `startup-config.cfg` file to the server.

Source	Destination	Description
nvram:backup-config	nvram:startup-config	Copies the backup configuration to the startup configuration.
nvram:clibanner	url	Copies the CLI banner to a server.
nvram:cpupktcapture.pcap	url	Uploads CPU packets capture file.
nvram:crash-log	url	Copies the crash log to a server.
nvram:errorlog	url	Copies the error log file to a server.
nvram:factory-defaults	url	Uploads factory defaults file.
nvram:log	url	Copies the log file to a server.
nvram:script <i>scriptname</i>	url	Copies a specified configuration script file to a server.

Fully Managed Switches M4250 and M4350 Series

Source	Destination	Description
<code>nvrām:startup-config</code>	<code>nvrām:backup-config</code>	Copies the startup configuration to the backup configuration.
<code>nvrām:startup-config</code>	<code>url</code>	Copies the startup configuration to a server.
<code>nvrām:traplog</code>	<code>url</code>	Copies the trap log file to a server.
<code>system:running-config</code>	<code>nvrām:startup-config</code>	Saves the running configuration to NVRAM.
<code>system:running-config</code>	<code>nvrām:factory-defaults</code>	Saves the running configuration to NVRAM to the <code>factory-defaults</code> file.
<code>nvrām:application sourcefilename</code>	<code>url</code>	Saves the source application file with the name specified by the <code>sourcefilename</code> argument.
<code>url</code>	<code>nvrām:application destfilename</code>	Downloads the source application file to the switch and saves it with the name specified by the <code>destfilename</code> argument.
<code>url</code>	<code>nvrām:ca-root index</code>	Downloads the CA certificate file to the switch. The CA certificate file is saved on the switch in the <code>CAindex.pem</code> format. For example, if you enter the <code>copy tftp://172.26.2.21/mycertificate.pem nvrām:ca-root 3</code> command, the CA certificate file is saved on switch with the name CA3.PEM.
<code>url</code>	<code>nvrām:clibanner</code>	Downloads the CLI banner to the system.
<code>url</code>	<code>nvrām:clientkey index</code>	Downloads the client key file to the switch. The client key file is saved on the switch in the <code>clientindex.key</code> format. For example, if you enter the <code>copy tftp://172.26.2.21/client.key nvrām:clientkey 4</code> command, the client key file is saved on switch with the name client4.key.
<code>url</code>	<code>nvrām:client-ssl-cert index</code>	Downloads the client certificate file to the switch. The client certificate file is saved on the switch in the <code>clientindex.pem</code> format. For example, if you enter the <code>copy tftp://172.26.2.21/client.pem nvrām:client-ssl-cert 2</code> command, the client key file is saved on switch with the name client2.pem.
<code>url</code>	<code>nvrām:factory-defaults</code>	Downloads the file as the factory default configuration.
<code>url</code>	<code>nvrām:publickey-config</code>	Downloads the Public Key for Configuration Script validation.
<code>url</code>	<code>nvrām:publickey-image</code>	Downloads Public Key for Image validation.

Fully Managed Switches M4250 and M4350 Series

Source	Destination	Description
<i>url</i>	<i>nvram:script destfilename</i>	Downloads a configuration script file to the system. During the download of a configuration script, the copy command validates the script. In case of any error, the command lists all the lines at the end of the validation process and prompts you to confirm before copying the script file.
<i>url</i>	<i>nvram:script destfilename noval</i>	When you use this option, the copy command does not validate the downloaded script file. An example of the CLI command follows: (NETGEAR Switch) #copy tftp://1.1.1.1/file.scr nvram:script file.scr noval
<i>url</i>	<i>nvram:sshkey-dsa</i>	Downloads an SSH key file. For more information, see Secure Shell Commands on page 85 .
<i>url</i>	<i>nvram:sshkey-rsa2</i>	Downloads an SSH key file.
<i>url</i>	<i>nvram:sslpem-dhweak</i>	Downloads an HTTP secure-server certificate.
<i>url</i>	<i>nvram:sslpem-dhstrong</i>	Downloads an HTTP secure-server certificate.
<i>url</i>	<i>nvram:sslpem-root</i>	Downloads an HTTP secure-server certificate. For more information, see Hypertext Transfer Protocol Commands on page 110 .
<i>url</i>	<i>nvram:sslpem-server</i>	Downloads an HTTP secure-server certificate.
<i>url</i>	<i>nvram:startup-config</i>	Downloads the startup configuration file to the system.
<i>url</i>	<i>ias-users</i>	Downloads an IAS users database file to the system. When the IAS users file is downloaded, the switch IAS user's database is replaced with the users and their attributes available in the downloaded file.
<i>url</i>	<i>{image1 image2}</i>	Download an image from the remote server to either image. The downloaded image is distributed to the stack members.
<i>url</i>	<i>nvram:tech-support-cmds</i>	Download the tech-support-cmds file to the switch. You can prepare a list of commands in this file. The tech-support infrastructure reads this file and displays the output of these additional commands if you issue the show tech-support command. This method is not supported under a subtree command such as the show tech-support dot3ad command.
<i>{image1 image2}</i>	<i>url</i>	Upload either image to the remote server.

Fully Managed Switches M4250 and M4350 Series

Source	Destination	Description
{image1 image2}	unit://unit/{image1 image2}	For an M4350 series switch, copy an image from the primary management unit to a specific member in a stack. Use the <code>unit</code> parameter to specify the member to which the image must be copied.
{image1 image2}	unit://*/{image1 image2}	For an M4350 series switch, copy an image from the primary management unit to all of members in a stack.

Command example:

The following example shows an ias users file that is downloaded and applied.

```
(NETGEAR Switch) #copy tftp://10.131.17.104/aaa_users.txt ias-users
```

```
Mode..... TFTP
Set Server IP..... 10.131.17.104
Path..... ./
Filename..... aaa_users.txt
Data Type..... IAS Users
```

```
Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
```

```
File transfer operation completed successfully.
```

```
Validating and updating the users to the IAS users database.
```

```
Updated IAS users database successfully.
```

file verify

M4250

M4350

This command enables digital signature verification while an image and/or configuration file is downloaded to the switch.

Format	file verify {all image none script}
Mode	Global Config
Parameter	Description
All	Verifies the digital signature of both image and configuration files.
Image	Verifies the digital signature of image files only.

Parameter	Description
None	Disables digital signature verification for both images and configuration files.
Script	Verifies the digital signature of configuration files.

no file verify

Resets the configured digital signature verification value to the factory default value.

Format	no file verify
Mode	Global Config

image verify

M4250

M4350

Use this command to validate an image file. The **file verify** command validates an image during download, whereas the **image verify** command validates an image in one of two partitions.

A digest of the image that is being validated is calculated and compared with a digest from the digital signature that was extracted (during download) of the same image. A match indicates a valid image.

Format	image verify {image1 image2}
Mode	Privileged EXEC

System Utility and Clear Commands

This section describes the commands you use to help troubleshoot connectivity issues and to restore various configurations to their factory defaults.

traceroute

M4250

M4350

Use the **traceroute** command to discover the routes that IPv4 or IPv6 packets actually take when traveling to their destination through the network on a hop-by-hop basis. Traceroute continues to provide a synchronous response when initiated from the CLI.

The user may specify the source IP address of the traceroute probes. Recall that traceroute works by sending packets that are expected not to reach their final destination, but instead trigger ICMP error messages back to the source address from each hop along the forward

path to the destination. By specifying the source address, the user can determine where along the forward path there is no route back to the source address. Note that this is only useful if the route from source to destination and destination to source is symmetric.) It would be common, for example, to send a traceroute from an edge router to a target higher in the network using a source address from a host subnet on the edge router. This would test reachability from within the network back to hosts attached to the edge router. Alternatively, one might send a traceroute with an address on a loopback interface as a source to test reachability back to the loopback interface address.

In the CLI, the user may specify the source either as an IPv4 address, IPv6 address, or as a routing interface. When the source is specified as a routing interface, the traceroute is sent using the primary IPv4 address on the source interface. With SNMP, the source must be specified as an address. The source cannot be specified in the web UI.

The switch does not accept an incoming packet that arrives on a routing interface if the packet's destination address is on one of the out-of-band management interfaces (service port or network port). An example of such a packet is a traceroute response. Similarly, the switch does not accept a packet that arrives on a management interface if the packet's destination is an address on a routing interface. Thus, it would be futile to send a traceroute on a management interface using a routing interface address as source, or to send a traceroute on a routing interface using a management interface as source. When sending a traceroute on a routing interface, the source must be that routing interface or another routing interface. When sending a traceroute on a management interface, the source must be on that management interface. For this reason, the user cannot specify the source as a management interface or management interface address. When sending a traceroute on a management interface, the user should not specify a source address, but instead let the system select the source address from the outgoing interface.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Default	count: 3 probes interval: 3 seconds size: 0 bytes port: 33434 maxTtl: 30 hops maxFail: 5 probes initTtl: 1 hop
Format	traceroute { <i>ip-address</i> [<i>ipv6</i>] { <i>ipv6-address</i> <i>hostname</i> }} [<i>initTtl initTtl</i>] [<i>maxTtl maxTtl</i>] [<i>maxFail maxFail</i>] [<i>interval interval</i>] [<i>count count</i>] [<i>port</i> <i>port</i>] [<i>size size</i>] [<i>source {ip-address ipv6-address unit/slot/port}</i>]
Mode	Privileged EXEC

Using the options described below, you can specify the initial and maximum time-to-live (TTL) in probe packets, the maximum number of failures before termination, the number of probes sent for each TTL, and the size of each probe.

Parameter	Description
ipaddress	The <i>ipaddress</i> value should be a valid IP address.
ipv6-address	The <i>ipv6-address</i> value should be a valid IPv6 address.
hostname	The <i>hostname</i> value should be a valid hostname.
ipv6	The optional ipv6 keyword can be used before <i>ipv6-address</i> or <i>hostname</i> . Giving the ipv6 keyword before the <i>hostname</i> tries it to resolve to an IPv6 address.
initTtl	Use initTtl to specify the initial time-to-live (TTL), the maximum number of router hops between the local and remote system. Range is 0 to 255.
maxTtl	Use maxTtl to specify the maximum TTL. Range is 1 to 255.
maxFail	Use maxFail to terminate the traceroute after failing to receive a response for this number of consecutive probes. Range is 0 to 255.
interval	Use the optional interval parameter to specify the time between probes, in seconds. If a response is not received within this interval, then traceroute considers that probe a failure (printing *) and sends the next probe. If traceroute does receive a response to a probe within this interval, then it sends the next probe immediately. Range is 1 to 60 seconds.
count	Use the optional count parameter to specify the number of probes to send for each TTL value. Range is 1 to 10 probes.
port	Use the optional port parameter to specify destination UDP port of the probe. This should be an unused port on the remote destination system. Range is 1 to 65535.
size	Use the optional size parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.
source	Use the optional source parameter to specify the source IP address or interface for the traceroute.

The following are examples of the CLI command.

Command example:

The following example shows that the traceroute is a success:

```
(NETGEAR Switch) # traceroute 10.240.10.115 initTtl 1 maxTtl 4 maxFail 0 interval 1 count
3 port 33434 size 43
```

```
Traceroute to 10.240.10.115 , 4 hops max 43 byte packets:
```

```
1 10.240.4.1    708 msec    41 msec    11 msec
2 10.240.10.115  0 msec      0 msec      0 msec
```

```
Hop Count = 1 Last TTL = 2 Test attempt = 6 Test Success = 6
```

Command example:

The following example shows that the IPv6 traceroute is a success:

```
(NETGEAR Switch) # traceroute 2001::2 initTtl 1 maxTtl 4 maxFail 0 interval 1 count 3
port 33434 size 43
```

Traceroute to 2001::2 hops max 43 byte packets:

```
1 2001::2    708 msec    41 msec    11 msec
```

The above command can also be execute with the optional ipv6 parameter as follows:

```
(NETGEAR Switch) # traceroute ipv6 2001::2 initTtl 1 maxTtl 4 maxFail 0 interval 1 count
3 port 33434 size 43
```

Command example:

The following example shows that the traceroute fails:

```
(NETGEAR Switch) # traceroute 10.40.1.1 initTtl 1 maxFail 0 interval 1 count 3
port 33434 size 43
```

Traceroute to 10.40.1.1 ,30 hops max 43 byte packets:

```
1 10.240.4.1    19 msec    18 msec    9 msec
```

```
2 10.240.1.252  0 msec     0 msec     1 msec
```

```
3 172.31.0.9    277 msec   276 msec   277 msec
```

```
4 10.254.1.1    289 msec   327 msec   282 msec
```

```
5 10.254.21.2   287 msec   293 msec   296 msec
```

```
6 192.168.76.2  290 msec   291 msec   289 msec
```

```
7 0.0.0.0      0 msec *
```

Hop Count = 6 Last TTL = 7 Test attempt = 19 Test Success = 18

Command example:

The following example shows that the IPv6 traceroute fails:

```
(NETGEAR Switch)# traceroute 2001::2 initTtl 1 maxFail 0 interval 1 count 3 port 33434
size 43
```

Traceroute to 2001::2 hops max 43 byte packets:

```
1 3001::1    708 msec    41 msec    11 msec
```

```
2 4001::2    250 msec    200 msec    193 msec
```

```
3 5001::3    289 msec    313 msec    278 msec
```

```
4 6001::4    651 msec    41 msec     270 msec
```

```
5          0          0 msec *
```

Hop Count = 4 Last TTL = 5 Test attempt = 1 Test Success = 0

clear config

M4250

M4350

This command resets the configuration to the factory defaults without powering off the switch. When you issue this command, a prompt appears to confirm that the reset should proceed.

When you enter *y*, you automatically reset the current configuration on the switch to the default values. It does not reset the switch.

You can also reset the configuration for a specific interface only.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>clear config [interface {<i>unit/slot/port</i> lag <i>lag-intf-num</i> loopback <i>loopback-id</i> vlan <i>vlan-id</i>}]</code>
Mode	Privileged EXEC

clear counters

M4250

M4350

This command clears the statistics for a specific port, for all ports, for a specific VLAN, for a specific LAG, or for the entire switch, based on the argument.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>clear counters {<i>unit/slot/port</i> all vlan <i>vlan-id</i> lag <i>lag-intf-num</i>}</code>
Mode	Privileged EXEC

clear mac-addr-table

M4250

M4350

This command clears the dynamically learned MAC addresses for all ports, for a specific port, for a specific VLAN, or for the entire switch, based on the argument. You can also clear a specific MAC address.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>clear mac-addr-table {all vlan <i>vlan-id</i> interface <i>unit/slot/port</i> <i>macaddr</i> [<i>macmask</i>] }</code>

Mode	Privileged EXEC

Parameter	Description
all	All dynamically learned forwarding database entries in the forwarding database table.
vlan-id	The dynamically learned forwarding database entries for the VLAN ID.
unit/slot/port	The dynamically learned forwarding database entries for the interface.
macaddr macmask	The dynamically learned forwarding database entries that match the range specified by the MAC address and MAC mask. If you do not specify the MAC mask, only the specified MAC address is removed from the forwarding database table.

clear igmpsnooping

M4250

M4350

This command clears the tables managed by the IGMP Snooping function and attempts to delete these entries from the Multicast Forwarding Database.

Format	<code>clear igmpsnooping</code>

Mode	Privileged EXEC

clear ip access-list counters

M4250

M4350

This command clears the counters of all or a specific IP ACL (which you can identify by either its ID or its name) or specific IP ACL rule.

Format	<code>clear ip access-list counters [{<i>acl-id</i> <i>acl-name</i>} [<i>rule-id</i>]]</code>

Mode	Privileged EXEC

clear mac access-list counters

M4250

M4350

This command clears the counters of all or a specific MAC ACL or specific MAC ACL rule.

Format	<code>clear mac access-list counters [acl-name [rule-id]]</code>

Mode	Privileged EXEC

clear ipv6 access-list counters

M4250

M4350

This command clears the counters of all or a specific IPv6 ACL or IPv6 ACL rule.

Format	<code>clear ipv6 access-list counters [acl-name [rule-id]]</code>

Mode	Privileged EXEC

clear traplog

M4250

M4350

This command clears the trap log.

Format	<code>clear traplog</code>

Mode	Privileged EXEC

clear vlan

M4250

M4350

This command resets VLAN configuration parameters to the factory defaults. When the VLAN configuration is reset to the factory defaults, GVRP and MVRP might be affected in the following situation:

1. Static VLANs are deleted.
2. GVRP is restored to the factory default as a result of handling the VLAN RESTORE NOTIFY event. Because GVRP is disabled by default, GVRP becomes disabled and all of its dynamic VLANs are deleted.
3. MVRP is restored to the factory default as a result of handling the VLAN RESTORE NOTIFY event. Because MVRP is enabled by default, any VLANs that were already created by MVRP are unaffected. However, for platforms on which MVRP is disabled by default, the

MVRP behavior must match GVRP. That is, MVRP is disabled and the MVRP VLANs are deleted.

Format	<code>clear vlan</code>

Mode	Privileged EXEC

logout

M4250

M4350

This command closes the current telnet connection or resets the current serial connection.

Note: Save configuration changes before logging out.

Format	<code>logout</code>

Modes	Privileged EXEC User EXEC

ping

M4250

M4350

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI and Web interfaces.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Note: For information about the **ping** command for IPv6 hosts, see [ping ipv6](#) on page 74.

Default	The default count is 1. The default interval is 3 seconds. The default size is 0 bytes.

Format	<code>ping {ip-address ipv6addr hostname ipv6 {ipv6-address hostname {interface {unit/slot/port vlan vlan-id loopback loopback-id serviceport} link-local-address}} [count count] [interval seconds] [size size] [source {ip-address ipv6addr unit/slot/port vlan vlan-id loopback loopback-id serviceport}] [outgoing-interface {unit/slot/port vlan vlan-id serviceport}]}</code>
Modes	Privileged EXEC User EXEC

Using the options described below, you can specify the number and size of echo requests and the interval between echo requests.

Parameter	Description
<i>ip-address</i>	The IPv4 address. You can set an IPv4 address as the destination and another IPv4 address as the source.
<i>ipv6address (or ipv6-address)</i>	The IPv6 address. You can set an IPv6 address as the destination and another IPv6 address as the source.
<i>hostname</i>	The host name. You can set a host name as the destination. If you use the ipv6 keyword, the host name resolves to an IPv6 address. Otherwise, the host name resolves to an IPv4 address.
<i>ipv6</i>	The optional keyword ipv6 can be used before the <i>ipv6-address</i> or <i>hostname</i> argument. Using the ipv6 optional keyword before <i>hostname</i> tries to resolve it directly to the IPv6 address. Also used for pinging a link-local IPv6 address.
<i>count count</i>	Use the count parameter to specify the number of ping packets (ICMP Echo requests) that are sent to the destination address. The range for <i>count</i> is 1 to 15 requests.
<i>interval seconds</i>	Use the interval parameter to specify the time between Echo Requests, in seconds. Range is 1 to 60 seconds.
<i>size size</i>	Use the size parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.
<i>interface</i>	Use the interface keyword to ping a link-local IPv6 address over an interface. The interface can be an interface number, a VLAN ID, a loopback ID, or the service port. You can also use the interface keyword to set the source interface
<i>link-local-address</i>	The link-local IPv6 address to ping over an interface.
<i>source</i>	The source IPv4 or IPv6 address or interface to use when sending the echo requests packets. The interface can be an interface number, a VLAN ID, a loopback ID, or the service port.
<i>outgoing-interface</i>	The outgoing interface to use when sending the echo requests packets. The outgoing interface can be an interface number, a VLAN ID, or the service port.

The following are examples of the CLI command.

Command example:

The following example shows that the IPv4 ping is a success:

```
(NETGEAR Switch) #ping 10.254.2.160 count 3 interval 1 size 255
Pinging 10.254.2.160 with 255 bytes of data:
```

```
Received response for icmp_seq = 0. time = 275268 usec
Received response for icmp_seq = 1. time = 274009 usec
Received response for icmp_seq = 2. time = 279459 usec
```

```
----10.254.2.160 PING statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 274/279/276
```

Command example:

The following example shows that the IPv6 ping is a success:

```
(NETGEAR Switch) #ping 2001::1
Pinging 2001::1 with 64 bytes of data:

Send count=3, Receive count=3 from 2001::1
Average round trip time = 3.00 ms
```

Command example:

The following example shows that the IPv4 ping fails because the destination cannot be reached:

```
(NETGEAR Switch) # ping 192.168.254.222 count 3 interval 1 size 255
Pinging 192.168.254.222 with 255 bytes of data:
Received Response: Unreachable Destination
Received Response :Unreachable Destination
Received Response :Unreachable Destination
----192.168.254.222 PING statistics----
3 packets transmitted,3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 0/0/0
```

Command example:

The following example shows that the IPv4 ping fails because the request times out:

```
(NETGEAR Switch) # ping 1.1.1.1 count 1 interval 3
Pinging 1.1.1.1 with 0 bytes of data:

----1.1.1.1 PING statistics----
1 packets transmitted,0 packets received, 100% packet loss
round-trip (msec) min/avg/max = 0/0/0
```

Command example:

The following example shows that the IPv6 ping fails:

```
(NETGEAR Switch) #ping ipv6 2001::4
Pinging 2001::4 with 64 bytes of data:
```

```
Send count=3, Receive count=0 from 2001::4
Average round trip time = 0.00 ms
```

ip scp server enable

M4250

M4350

This command enables SCP server functionality for SCP push operations on the switch, which allows files to be transferred from the host device to the switch using the SCP protocol. During an SCP file transfer operation, the management operations on the switch are blocked. After the completion of file download to the switch, the switch performs file validations similar to other download operations executed using the `copy` command.

To allow the SCP file transfers from the host system to the switch, you must enable the SCP server on the switch.

Default	Disabled
Format	ip scp server enable
Mode	Privileged EXEC

The transfer is initiated using the CLI on the host system, and not from the switch CLI. The following examples show the syntax for SCP push commands executed on a PC host for configuration and firmware images:

- scp <config file> user@<scp server IP>:startup-config
- scp <config file> user@<scp server IP>:backup-config
- scp <config file> user@<scp server IP>:factory-defaults
- scp <config file> user@<scp server IP>:<scriptfile.scr>
- scp <image file> user@<scp server IP>:active
- scp <image file> user@<scp server IP>:backup

no ip scp server enable

This command resets the SCP server functionality for SCP push operations on the switch to the default value (disabled).

Format	no ip scp server enable
Modes	Privileged EXEC

quit

M4250**M4350**

This command closes the current telnet connection or resets the current serial connection. The system asks you whether to save configuration changes before quitting.

Format	quit
Modes	Privileged EXEC User EXEC

reload (Privileged EXEC)

M4250**M4350**

This command resets the switch without powering it off. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. The LEDs on the switch indicate a successful reset.

Format	reload
Mode	Privileged EXEC

reload configuration

M4250**M4350**

This command gracefully reloads the configuration. If you do not specify a script name, the switch reloads the existing startup-config file. If you specify a script name, you must include the extension.

Format	reload configuration [<i>scriptname</i>]
Mode	Privileged EXEC

write memory

M4250**M4350**

Use this command to save running configuration changes to NVRAM so that the changes you make will persist across a reboot. This command is the same as **copy system:running-config nvram:startup-config**. Use the **confirm** keyword to directly save the configuration to NVRAM without prompting for a confirmation.

Format	<code>write memory [confirm]</code>

Mode	Privileged EXEC

dying gasp

M4250

M4350

This command causes a dying-gasp notification to be sent through the syslog if the switch loses power or resets abruptly. The switch reset might be due to an unexpected software failure, a LOG_ERROR, or a user-triggered switch reload. The Dying Gasp feature also notifies dying gasp events as an SNMP trap to the trap receiver

The ability to send a dying-gasp notification on loss of power depends on the platform hardware capability. The switch hardware must be able to supply back power for approximately 300 ms to send the dying gasp notification after the abrupt power loss or reset occurs.

Format	<code>dying-gasp primary {syslog snmptrap} secondary {syslog snmptrap}</code>

Mode	Global Config

Parameter	Description
primary	The Dying Gasp primary notification
secondary	The Dying Gasp secondary notification
syslog	Logs an entry in the syslog
snmptrap	Sends an SNMP trap

show dying-gasp status

M4250

M4350

This command displays the dying gasp configuration status.

Format	<code>show dying-gasp status</code>

Mode	Privileged EXEC

Parameter	Description
Dying Gasp Primary Mode	Identifies the primary notification mode, which can be one of the following: • Syslog • SnmpTrap
Dying Gasp Secondary Mode	Identifies the secondary notification mode, which can be one of the following: • Syslog • SnmpTrap

Network Time Protocol Commands

Network Time Protocol (NTP) is used for synchronization of the system time. The switch supports the client-side configurations of NTP.

ntp authenticate

M4250

M4350

This command enables NTP authentication.

Default	Disabled
Format	ntp authenticate
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config) #ntp authenticate
```

no ntp authenticate

This command disables NTP authentication.

Format	no ntp authenticate
Mode	Global Config

ntp authentication-key

M4250**M4350**

This command configures the authentication key and the SHA-2 algorithm for a trusted NTP time source, and requires you to set a new password for NTP authentication. The NTP authentication key number must be unique across the switch.

Default	SHA2
Format	<code>ntp authentication-key <i>key-number</i> sha2 [<i>encrypted key-name</i>]</code>
Mode	Global Config
Parameter	Description
<i>key-number</i>	The number for identifying an authentication key. The range is from 1 to 4,294,967,295.
<i>key-name</i>	The encrypted key-value. This is an optional setting.

Command example:

```
(NETGEAR Switch) (Config) #ntp authentication-key 81 sha2
Enter new password:*****
Confirm new password:*****
```

no ntp authentication-key

This command deletes a configured authentication key.

Format	<code>no ntp authentication-key <i>key-number</i></code>
Mode	Global Config

ntp trusted-key

M4250**M4350**

This command designates one or more authentication keys from the configured list as the trusted key for client-server communication.

Default	None
Format	<code>ntp trusted-key {<i>key-number</i> <i>key-number-list</i>}</code>
Mode	Global Config

Parameter	Description
<i>key-number</i>	The number for identifying an authentication key. The range is from 1 to 4,294,967,295.
<i>key-number-list</i>	The comma-separated list of authentication keys. For each key, the range is from 1 to 4,294,967,295.

Command example:

```
(NETGEAR Switch) (Config) #ntp trusted-key 81
```

Command example:

```
(NETGEAR Switch) (Config) #ntp trusted-key 1,5,7
```

```
no ntp trusted-key
```

This command deletes one or more configured trusted keys.

Format	<code>no ntp trusted-key {key-number key-number-list}</code>
Mode	Global Config

```
ntp broadcast client
```

M4250

M4350

This command configures the NTP client to run as a broadcast client, allowing the client to receive broadcast packets.

Default	Disabled
Format	<code>ntp broadcast client</code>
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config) #ntp broadcast client
```

```
no ntp broadcast client
```

This command disables the broadcast client mode.

Format	<code>no ntp broadcast client</code>
Mode	Global Config

ntp broadcastdelay

M4250**M4350**

This command sets the estimated round-trip delay in microseconds between an NTP client and an NTP broadcast server. The delay is applicable only when the client is configured in broadcast mode. The delay can be from 1 to 999,999 microseconds.

Default	3000
Format	<code>ntp broadcastdelay microseconds</code>
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config)#ntp broadcastdelay 10000
```

no ntp broadcast client

This command resets the estimated round-trip delay in microseconds between an NTP client and an NTP broadcast server to the default.

Format	<code>no ntp broadcastdelay</code>
Mode	Global Config

ntp server

M4250**M4350**

This command configures the NTP server to allow the system clock to be synchronized by a time server. You can configure multiple NTP servers. The server selection algorithm settles on the server for time synchronization.

Configuring a preferred status overrides the algorithm and the configured server is used for time synchronization. Configuring a preferred server reduces switching back and forth among servers. The preferred status indicates if an NTP server is the preferred server if two servers show different times, which is meaningful only if you configure two NTP servers. If you

configure three or more NTP servers, the NTP function automatically finds the most reliable server.

Default	No NTP server configured The NTP version is 4. The minimum polling interval is 64 seconds. The maximum polling interval is 1024seconds.
Format	<code>ntp server server-address [version number] [key key-id] [minpoll interval] [maxpoll interval] [prefer] [burst] [iburst]</code>
Mode	Global Config

Parameter	Description
<i>server-address</i>	The server IPv4 address, IPv6 address, or host name for the client to synchronize time with. The host name range is from 1 to 256 characters.
<i>version number</i>	The protocol version. The default is 4. The range is 1 to 4.
<i>key key-id</i>	The Authentication key, which can be from 1 to 4,294,967,295.
<i>minpoll interval</i>	The minimum polling interval in seconds as a power of 2. The range is from 4 to 17, which in seconds is 16 seconds to 131,072 seconds. The default is 64 seconds.
<i>maxpoll interval</i>	The maximum polling interval in seconds as a power of 2. The range is from 4 to 17, which in seconds is 16 seconds to 131,072 seconds. The default is 1024 seconds.
<i>prefer</i>	The server is a preferred server in the server selection. This is an optional setting.
<i>burst</i>	Within each synchronization interval, a series of packets instead of a single packet is sent. This method achieve faster synchronization. This is an optional setting.
<i>iburst</i>	During the initial synchronization interval, a series of packets instead of a single packet is sent. This method achieve faster initial synchronization. This is an optional setting.

Command example:

```
(NETGEAR Switch) (Config) #ntp server 1.1.1.1
```

`no ntp server`

This command deletes a configured NTP server.

Format	<code>no ntp server server-address</code>
Mode	Global Config

ntp source-interface

M4250

M4350

This command configures the NTP source interface.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Default	None
Format	<code>ntp source-interface [unit/slot/port loopback interface-id serviceport vlan vlan-id]</code>
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config) #ntp source-interface vlan 45
```

no ntp source-interface

This command deletes the NTP source-interface configuration.

Format	<code>no ntp source-interface</code>
Mode	Global Config

show ntp

M4250

M4350

This command displays the global NTP configuration settings.

Format	<code>show ntp</code>
Mode	Privileged Config

Fields	Description
NTP Broadcast Client Mode	The NTP broadcast client mode (Disabled or Enabled).
NTP Authentication Mode	The NTP authentication mode (Disabled or Enabled).
Broadcast Delay	The delay in microseconds, that is, the delay in receiving broadcast packets from the server.

Fields	Description
Source Interface	The source interface that is used in NTP client communication with the server.
Source IPv4 Address	The source IPv4 address (if configured).
Source IPv6 Address	The source IPv6 address (if configured).
VRF Name	The VRF instance that the client is associated with.

Command example:

```
(NETGEAR Switch) #show ntp
```

```
NTP Broadcast Client Mode ..... Disabled
NTP Authentication Mode ..... Enabled
Broadcast Delay ..... 3000
Source Interface..... 1/0/5
Source IPv4 Address..... 1.2.3.4
Source IPv6 Address..... ::
VRF Name..... test
```

show ntp authentication-keys**M4250****M4350**

This command displays information about the configured NTP authentication keys.

Format	show ntp authentication-keys
Mode	Privileged Config

Fields	Description
Key Id	The specified authentication key.
Key Value	The configured key value (encrypted).
Message Authentication Algorithm	By default, the authentication algorithm is SHA2.
Trusted	Indicates if the keys are trusted (Yes or No).

Command example:

```
(NETGEAR Switch) #show ntp authentication-keys
```

```
Key Id ..... 1
Key Value ..... 66f7e003db45a5f4688fd3a7ee7112df
```

```

Message Authentication Algorithm ..... sha2
Trusted ..... Yes

Key Id ..... 2
Key Value ..... 66f7e003db45a5f4688fd3a7ee7112df
Message Authentication Algorithm ..... sha2
Trusted ..... No

```

show ntp servers

M4250

M4350

This command displays information about the configured NTP servers.

Format	show ntp servers
Mode	Privileged Config
Fields	Description
Address	The IP address of the NTP server.
Version	The protocol version that the server is running.
Key Id	The authentication ID.
Minimum Poll Interval	The minimum polling interval in seconds as a power of 2.
Maximum Poll Interval	The maximum polling interval in seconds as a power of 2.
Prefer	The preference status for this server in the selection algorithm.
Burst	Indicates if a series of packets are sent instead of a single packet.
Iburst	Indicates if a series of packets are sent instead of a single packet during initial synchronization.

Command example:

```
(NETGEAR Switch)#show ntp servers
```

```

Address ..... time-a.netgear.com
Version ..... 4
Key Id ..... 0
Minimum Poll Interval ..... 6
Maximum Poll Interval ..... 10
Prefer ..... No
Burst ..... Yes
Iburst ..... Yes

```



```

Address ..... time-c.netgear.com
Version ..... 4
Key Id ..... 0
Minimum Poll Interval ..... 6
Maximum Poll Interval ..... 10
Prefer ..... No
Burst ..... Yes
Iburst ..... Yes

```

show ntp status

M4250

M4350

This command displays the NTP synchronization status.

Format	show ntp servers
Mode	Privileged Config

The following table displays the most significant fields in the command output.

Fields	Description
associd	The association identifier.
status	The status string with the client protocol status.
leap indicator	A 2-bit integer warning of an impending leap second to be inserted or deleted in the last minute of the current month.
stratum	An 8-bit integer indicating the stratum level of the local clock.
log2 precision	The precision of the local clock, in seconds to the nearest power of two.
root delay	The round trip delay to the reference clock.
root dispersion	The dispersion to the reference clock.
reference ID	The code identifying the particular server or reference clock.

Command example:

```
(NETGEAR Switch)#show ntp status
```

```

associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync,
system peer:      ec2-52-20-169-152.compute-1.amazonaws.com:123
system peer mode:  client
leap indicator:    00
stratum:          6
log2 precision:    -22

```

Fully Managed Switches M4250 and M4350 Series

```
root delay:          123.264
root dispersion:     47.976
reference ID:        0x3414a998
reference time:      ead8f175.758c4e24  Fri, Nov  8 2024 20:22:13.459
system jitter:       2.734566
clock jitter:        0.868
clock wander:        0.036
broadcast delay:     -50.000
symm. auth. delay:  0
```

show ntp packets

M4250

M4350

Use this command to display the global statistics for the NTP packets.

Format	show ntp packets
Mode	Privileged Config

Fields	Description
Ntp In packets	The number of packets received by the client.
Ntp Out packets	The number of packets transmitted by the client.
Ntp old version packets	The number of packets that do not match the running version of the protocol.
Ntp protocol error packets	The number of packets received that fail protocol validation checks.

Command example:

```
(NETGEAR Switch)#show ntp packets

Ntp In packets ..... 6609
Ntp Out packets ..... 6604
Ntp old version packets ..... 0
Ntp protocol error packets ..... 0
```

show ntp associations

M4250

M4350

This command displays the NTP associations, and optionally per-association details or per-association statistics.

Format	show ntp associations [detail statistics]

Mode	Privileged Config

Command example:

```
(NETGEAR Switch)#show ntp associations
```

remote	refid	st	t	when	poll	reach	delay	offset	jitter
+54.111.222.33	54.90.191.9	5	u	884	1024	377	122.570	+0.384	0.571
*52.222.111.35	54.81.127.33	5	u	143	1024	377	122.093	-1.046	0.692

Command example:

```
(NETGEAR Switch)#show ntp associations detail
```

```
associd=54556 status=941d conf, reach, sel_candidate, 1 event, popcorn,
srcadr=ec2-54-156-236-53.compute-1.amazonaws.com, srcport=123,
dstadr=172.22.10.183, dstport=123, received=3307, sent=3360, badauth=0,
seldisp=0, selbroken=0, leap=00, stratum=5, precision=-21,
rootdelay=1.022, rootdisp=13.718, refid=0x365abf09,
reftime=ead8fc96.59076f7f Fri, Nov 8 2024 21:09:42.347,
rec=ead8ff47.74d14dff Fri, Nov 8 2024 21:21:11.456, reach=377,
unreach=0, hmode=3, pmode=4, hpoll=10, ppoll=10, headway=0, flash=00 ok,
keyid=0, offset=+0.384, delay=122.570, dispersion=0.064, jitter=0.571,
xleave=0.043,
filtldelay= 122.70 123.84 125.06 122.57 127.97 126.27 138.52 130.95,
filtoffset= +0.30 +0.20 +1.49 +0.38 -0.53 +0.01 +0.60 +0.27,
filtldisp= 0.00 0.03 0.06 0.09 0.12 0.15 0.18 0.21
```

```
associd=54557 status=96fa conf, reach, sel_sys.peer, 15 events, sys_peer,
srcadr=ec2-52-20-169-152.compute-1.amazonaws.com, srcport=123,
dstadr=172.22.10.183, dstport=123, received=3305, sent=3373, badauth=0,
seldisp=0, selbroken=0, leap=00, stratum=5, precision=-25,
rootdelay=0.626, rootdisp=0.183, refid=0x36517f21,
reftime=ead9021b.cd6620d7 Fri, Nov 8 2024 21:33:15.802,
rec=ead9022c.74b4c37f Fri, Nov 8 2024 21:33:32.455, reach=377,
unreach=0, hmode=3, pmode=4, hpoll=10, ppoll=10, headway=299,
```

Command example:

```
(NETGEAR Switch)#show ntp associations statistics
```

```
Association ..... 54556
Ntp In packets ..... 3307
Ntp Out packets ..... 3360
Ntp protocol error packets ..... 0
```

```
Association ..... 54557
Ntp In packets ..... 3305
Ntp Out packets ..... 3373
Ntp protocol error packets ..... 0
```

show ntp information**M4250****M4350**

This command displays the NTP software information. The output fields are self-explanatory.

Format	show ntp information

Mode	Privileged Config

Command example:

```
(NETGEAR Switch)#show ntp information
```

```
Ntp Software Name ..... ntpd
Ntp Software Version ..... ntpd 4.2.8p17@1.4004-o
Ntp System Type ..... Linux/4.14.174-ldk_6.x-4d296fa3
```

Time Zone Commands

Use the time zone commands to configure system time and date, time zone, and summer time (that is, daylight saving time). Summer time can be recurring or non-recurring.

clock set

M4250

M4350

This command sets the system time and date.

Format	<code>clock set hh:mm:ss</code> <code>clock set mm/dd/yyyy</code>
Mode	Global Config
Parameter	Description
hh:mm:ss	Enter the current system time in 24-hour format in hours, minutes, and seconds. The range is hours: 0 to 23, minutes: 0 to 59, seconds: 0 to 59.
mm/dd/yyyy	Enter the current system date the format month, day, year. The range for month is 1 to 12. The range for the day of the month is 1 to 31. The range for year is 2010 to 2079.

Command example:

```
(NETGEAR Switch) (Config)# clock set 03:17:00
(NETGEAR Switch) (Config)# clock set 11/01/2011
```

clock summer-time date

M4250

M4350

Use the clock summer-time date command to set the summer-time offset to Coordinated Universal Time (UTC). If the optional parameters are not specified, they are read as either 0 or \0, as appropriate.

Format	<code>clock summer-time date {date month year hh:mm date month year hh:mm} [offset offset] [zone acronym]</code>
Mode	Global Config
Parameter	Description
date	Day of the month. Range is 1 to 31.
month	Month. Range is the first three letters by name; jan, for example.

Parameter	Description
year	Year. The range is 2000 to 2097.
hh:mm	Time in 24-hour format in hours and minutes. The range is hours: 0 to 23, minutes: 0 to 59.
offset	The number of minutes to add during the summertime. The range is 1 to 1440.
acronym	The acronym for the summer-time to be displayed when summertime is in effect. The range is up to four characters are allowed.

Command example:

```
(NETGEAR Switch) (Config)# clock summer-time date 1 nov 2011 3:18 2 nov 2011 3:18
(NETGEAR Switch) (Config)# clock summer-time date 1 nov 2011 3:18 2 nov 2011 3:18 offset
120 zone INDA
```

clock summer-time recurring

M4250**M4350**

This command sets the summer-time recurring parameters.

Format	<code>clock summer-time recurring {week day month hh:mm week day month hh:mm} [offset offset] [zone acronym]</code>
Mode	Global Config

Parameter	Description
EU	The system clock uses the standard recurring summer time settings used in countries in the European Union.
USA	The system clock uses the standard recurring daylight saving time settings used in the United States.
week	Week of the month. The range is 1 to 5, first, last.
day	Day of the week. The range is the first three letters by name; sun, for example.
month	Month. The range is the first three letters by name; jan, for example.
hh:mm	Time in 24-hour format in hours and minutes. The range is hours: 0 to 23, minutes: 0 to 59.
offset	The number of minutes to add during the summertime. The range is 1 to 1440.
acronym	The acronym for the summertime to be displayed when summertime is in effect. Up to four characters are allowed.

Command example:

```
(NETGEAR Switch) (Config)# clock summer-time recurring 2 sun nov 3:18 2 mon nov 3:18
(NETGEAR Switch) (Config)# clock summer-time recurring 2 sun nov 3:18 2 mon nov 3:18
offset 120 zone INDA
```

no clock summer-time

This command disables the summer time settings.

Format	no clock summer-time

Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config)# no clock summer-time
```

clock timezone

M4250

M4350

Use this command to set the offset to Coordinated Universal Time (UTC). If the optional parameters are not specified, they will be read as either 0 or \0 as appropriate.

Format	clock timezone {hours} [minutes minutes] [zone acronym]

Mode	Global Config

Parameter	Description
hours	Hours difference from UTC. The range is -12 to +13.
minutes	Minutes difference from UTC. The range is 0 to 59.
acronym	The acronym for the time zone. The range is up to four characters.

Command example:

```
(NETGEAR Switch) (Config)# clock timezone 5 minutes 30 zone INDA
```

no clock timezone

Use this command to reset the time zone settings.

Format	no clock timezone

Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config)# no clock timezone
```

show clock

M4250

M4350

Use this command to display the time and date from the system clock.

Format	show clock

Mode	Privileged Exec

Command example:

```
(NETGEAR Switch) # show clock
15:02:09 (UTC+0:00) Nov 1 2011
No time source
```

Command example:

```
(NETGEAR Switch) # show clock
10:55:40 INDA(UTC+7:30) Nov 1 2011
No time source
```

show clock detail

M4250

M4350

Use this command to display the detailed system time along with the time zone and the summertime configuration.

Format	show clock detail

Mode	Privileged Exec

Command example:

```
(NETGEAR Switch) # show clock detail

15:05:24 (UTC+0:00) Nov 1 2011
No time source

Time zone:
Acronym not configured
Offset is UTC+0:00

Summertime:
Summer-time is disabled
```


Command example:

```
((NETGEAR Switch) # show clock detail

10:57:57 INDA(UTC+7:30) Nov 1 2011
No time source

Time zone:
Acronym is INDA
Offset is UTC+5:30

Summertime:
Acronym is INDA
Recurring every year
Begins on second Sunday of Nov at 03:18
Ends on second Monday of Nov at 03:18
Offset is 120 minutes
Summer-time is in effect.
```

DHCP Server Commands

This section describes the commands you to configure the DHCP server settings for the switch. DHCP uses UDP as its transport protocol and supports a number of features that facilitate in administration address allocations.

ip dhcp pool

M4250

M4350

This command configures a DHCP address pool name on a DHCP server and lets the CLI enter the DHCP pool configuration mode.

Default	none
Format	ip dhcp pool <i>name</i>
Mode	Global Config

no ip dhcp pool

This command removes the DHCP address pool. The name should be previously configured pool name.

Format	no ip dhcp pool <i>name</i>

Mode	Global Config

client-identifier (DHCP Pool Config)

M4250

M4350

This command specifies the unique identifier for a DHCP client. Unique-identifier is a valid notation in hexadecimal format. In some systems, such as Microsoft DHCP clients, the client identifier is required instead of hardware addresses. The unique-identifier is a concatenation of the media type and the MAC address. For example, the Microsoft client identifier for Ethernet address c819.2488.f177 is 01c8.1924.88f1.77 where 01 represents the Ethernet media type. For more information, refer to the “Address Resolution Protocol Parameters” section of RFC 1700, Assigned Numbers for a list of media type codes.

Default	none

Format	client-identifier <i>uniqueidentifier</i>

Mode	DHCP Pool Config

no client-identifier

This command deletes the client identifier.

Format	no client-identifier

Mode	DHCP Pool Config

client-name (DHCP Pool Config)

M4250

M4350

This command specifies the name for a DHCP client. Name is a string consisting of standard ASCII characters.

Default	none

Format	client-name <i>name</i>

Mode	DHCP Pool Config

no client-name

This command removes the client name.

Format	no client-name

Mode	DHCP Pool Config

default-router (DHCP Pool Config)

M4250

M4350

This command specifies the default router list for a DHCP client. *address1*, *address2*...*address8* are valid IP addresses, each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	none

Format	default-router <i>address1</i> [<i>address2</i> <i>address8</i>]

Mode	DHCP Pool Config

no default-router

This command removes the default router list.

Format	no default-router

Mode	DHCP Pool Config

dns-server (DHCP Pool Config)

M4250

M4350

This command specifies the IP servers available to a DHCP client. Address parameters are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	none

Format	dns-server <i>address1</i> [<i>address2</i> <i>address8</i>]

Mode	DHCP Pool Config

no dns-server

This command removes the DNS Server list.

Format	no dns-server
Mode	DHCP Pool Config

hardware-address (DHCP Pool Config)

M4250

M4350

This command specifies the hardware address of a DHCP client. Hardware-address is the MAC address of the hardware platform of the client consisting of 6 bytes in dotted hexadecimal format. Type indicates the protocol of the hardware platform. It is 1 for 10 MB Ethernet and 6 for IEEE 802.

Default	ethernet
Format	hardware-address <i>hardwareaddress type</i>
Mode	DHCP Pool Config

no hardware-address

This command removes the hardware address of the DHCP client.

Format	no hardware-address
Mode	DHCP Pool Config

host (DHCP Pool Config)

M4250

M4350

This command specifies the IP address and network mask for a manual binding to a DHCP client. Address and Mask are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. The prefix-length is an integer from 0 to 32.

Default	none
Format	host <i>address [mask prefix-length]</i>
Mode	DHCP Pool Config

no host

This command removes the IP address of the DHCP client.

Format	no host

Mode	DHCP Pool Config

lease (DHCP Pool Config)

M4250

M4350

This command configures the duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client. The overall lease time must be between 1—86400 minutes. If you specify **infinite**, the lease is set for 60 days. You can also specify a lease duration: *days* is an integer from 0 to 59; *hours* is an integer from 0 to 23; *minutes* is an integer from 0 to 59.

Default	1 (day)

Format	lease [{ <i>days</i> [<i>hours</i>] [<i>minutes</i>] infinite}]

Mode	DHCP Pool Config

no lease

This command restores the default value of the lease time for DHCP Server.

Format	no lease

Mode	DHCP Pool Config

network (DHCP Pool Config)

M4250

M4350

Use this command to configure the subnet number and mask for a DHCP address pool on the server. Network-number is a valid IP address, made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. Mask is the IP subnet mask for the specified address pool. The prefix-length is an integer from 0 to 32.

Default	none

Format	network <i>networknumber</i> [<i>mask</i> <i>prefixlength</i>]

Mode	DHCP Pool Config

no network (DHCP Pool Config)

This command removes the subnet number and mask.

Format	no network
Mode	DHCP Pool Config

bootfile (DHCP Pool Config)

M4250

M4350

The command specifies the name of the default boot image for a DHCP client. The *filename* specifies the boot image file.

Format	bootfile filename
Mode	DHCP Pool Config

no bootfile (DHCP Pool Config)

This command deletes the boot image name.

Format	no bootfile
Mode	DHCP Pool Config

domain-name (DHCP Pool Config)

M4250

M4350

This command specifies the domain name of a Domain Name System (DNS) server for a DHCP client when the DHCP server allocates an IP address to the client. That is, the domain name is issued to the DHCP client, not to the switch.

The *domain* specifies the domain name for the DHCP client.

Default	none
Format	domain-name domain
Mode	DHCP Pool Config

no domain-name

This command removes the domain name of a DNS server for a DHCP client.

Format	no domain-name

Mode	DHCP Pool Config

netbios-name-server (DHCP Pool Config)

M4250

M4350

This command configures NetBIOS Windows Internet Naming Service (WINS) name servers that are available to DHCP clients.

One IP address is required, although one can specify up to eight addresses in one command line. Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Default	none

Format	netbios-name-server address [address2...address8]

Mode	DHCP Pool Config

no netbios-name-server

This command removes the NetBIOS name server list.

Format	no netbios-name-server

Mode	DHCP Pool Config

netbios-node-type (DHCP Pool Config)

M4250

M4350

The command configures the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients. The *type* argument specifies the NetBIOS node type. Valid types are:

- **b-node.** Broadcast
- **p-node.** Peer-to-peer
- **m-node.** Mixed
- **h-node.** Hybrid (recommended)

Default	none
Format	netbios-node-type <i>type</i>
Mode	DHCP Pool Config

no netbios-node-type

This command removes the NetBIOS node Type.

Format	no netbios-node-type
Mode	DHCP Pool Config

next-server (DHCP Pool Config)

M4250

M4350

This command configures the next server in the boot process of a DHCP client. The *address* parameter is the IP address of the next server in the boot process, which is typically a TFTP server.

Default	inbound interface helper addresses
Format	next-server <i>address</i>
Mode	DHCP Pool Config

no next-server

This command removes the boot server list.

Format	no next-server
Mode	DHCP Pool Config

option (DHCP Pool Config)

M4250

M4350

The **option** command configures DHCP Server options. The *code* parameter specifies the DHCP option code and ranges from 1-254. The *ascii string* parameter specifies an NVT ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks. The *hex string* parameter specifies hexadecimal data. In hexadecimal, character strings are two hexadecimal digits. You can separate each byte by a period (for example, a3.4f.22.0c), colon (for example, a3:4f:22:0c), or white space (for example, a3 4f 22 0c).

Default	none
Format	<code>option code {ascii string hex string1 [string2...string8] ip address1 [address2...address8]}</code>
Mode	DHCP Pool Config

no option

This command removes the DHCP Server options. The *code* parameter specifies the DHCP option code.

Format	<code>no option code</code>
Mode	DHCP Pool Config

auto-default-router (DHCP Pool Config)

M4250

M4350

This command enables automatic transmission of the interface IP address as the default-gateway.

Default	none
Format	<code>auto-default-router</code>
Mode	DHCP Pool Config

no auto-default-router

This command disables automatic transmission of the interface IP address as the default-gateway.

Format	<code>no auto-default-router</code>
Mode	DHCP Pool Config

ntp (DHCP Pool Config)

M4250**M4350**

This command configures the IP address of an NTP server in the boot process of a DHCP client. As an option, you can configure the IP address of a secondary NTP server.

Default	none
Format	ntp <i>ip-address1</i> [<i>ip-address2</i>]
Mode	DHCP Pool Config

no ntp

This command removes all IP addresses of NTP servers in the boot process of a DHCP client.

Format	no ntp
Mode	DHCP Pool Config

domain-name

M4250**M4350**

This command specifies the domain name of a DNS server that the switch sends to the RADIUS server for authentication. Use this command in combination with the **domain-name enable** command.

The *name* argument specifies the domain name.

Default	none
Format	domain-name <i>name</i>
Mode	Global Config

no domain-name

This command removes the domain name of a DNS server that the switch sends to the RADIUS server.

Format	no domain-name <i>name name</i>
Mode	Global Config

domain-name enable

M4250**M4350**

This command enables the switch to send the domain name of a DNS server that you specify with the **domain-name** command to a RADIUS server. By default, the switch sends only the domain name of the DNS server.

Default	Disabled
Format	domain-name enable
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config)#domain-name enable
(NETGEAR Switch) (Config)#exit
```

no domain-name enable

This command disables sending of the domain name of a DNS server to a RADIUS server.

Format	no domain-name enable
Mode	Global Config

ip dhcp excluded-address

M4250**M4350**

This command specifies the IP addresses that a DHCP server should not assign to DHCP clients. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	none
Format	ip dhcp excluded-address <i>low-address</i> [<i>high-address</i>]
Mode	Global Config

no ip dhcp excluded-address

This command removes the excluded IP addresses for a DHCP client. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Format	no ip dhcp excluded-address <i>low-address</i> [<i>high-address</i>]

Mode	Global Config

ip dhcp ignore-client-identifier

M4250

M4350

This command specifies that DHCP Option 61 (the client identifier) must be ignored.

Default	none

Format	ip dhcp ignore-client-identifier

Mode	Global Config

no ip dhcp ignore-client-identifier

This command specifies that DHCP Option 61 (the client identifier) cannot be ignored.

Format	no ip dhcp ignore-client-identifier

Mode	Global Config

ip dhcp ping packets

M4250

M4350

Use this command to specify the number, in a range from 2–10, of packets a DHCP server sends to a pool address as part of a ping operation. By default the number of packets sent to a pool address is 2, which is the smallest allowed number when sending packets. Setting the number of packets to 0 disables this command.

Default	2

Format	ip dhcp ping packets <i>number</i>

Mode	Global Config

no ip dhcp ping packets

This command restores the number of ping packets to the default value.

Format	no ip dhcp ping packets

Mode	Global Config

service dhcp

M4250

M4350

This command enables the DHCP server.

Default	disabled

Format	service dhcp

Mode	Global Config

no service dhcp

This command disables the DHCP server.

Format	no service dhcp

Mode	Global Config

ip dhcp bootp automatic

M4250

M4350

This command enables the allocation of the addresses to the bootp client. The addresses are from the automatic address pool.

Default	disabled

Format	ip dhcp bootp automatic

Mode	Global Config

no ip dhcp bootp automatic

This command disables the allocation of the addresses to the bootp client. The address are from the automatic address pool.

Format	no ip dhcp bootp automatic

Mode	Global Config

ip dhcp conflict logging

M4250**M4350**

This command enables conflict logging on DHCP server.

Default	enabled
Format	ip dhcp conflict logging
Mode	Global Config

no ip dhcp conflict logging

This command disables conflict logging on DHCP server.

Format	no ip dhcp conflict logging
Mode	Global Config

ip dhcp class

M4250**M4350**

This command defines a DHCP class with Option-82 through circuit ID and remote ID suboptions. If you configure a DHCP class in the Global Config mode, you can bind the DHCP class is under multiple DHCP pools.

When you define a DHCP class in the Global Config mode, the CLI enters the DHCP Class Config mode.

Default	none
Format	ip dhcp class <i>name</i>
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config)#ip dhcp class Class1
(NETGEAR Switch) (Config-dhcp-class)#
```

no ip dhcp class

This command removes a DHCP class

Format	no ip dhcp class <i>name</i>
Mode	Global Config

relay agent information remote-id circuit-id (DHCP Class Config)

M4250

M4350

This command defines DHCP classes with Option-82 through circuit ID and remote ID suboptions. Each DHCP server class is configured with Option-82 (both remote ID and circuit ID). The circuit ID configuration is optional.

Default	None
Format	relay agent information remote-id <i>remote-string</i> [circuit-id <i>circuit-string</i>]
Mode	DHCP Class Config

Parameter	Definition
<i>remote-string</i>	The remote ID configured on the DHCP L2 relay to which the DHCP client is connected.
<i>circuit-string</i>	The interface number in the unit/slot/port format to which the DHCP client is connected.

Command example:

```
(NETGEAR Switch) (Config) #ip dhcp class Class1
(NETGEAR Switch) (Config-dhcp-class) #relay agent information remote-id COACH1 circuit-id
1/0/13
```

no relay agent information remote-id circuit-id

This command removes the relay agent information from the DHCP class.

Format	no relay agent information remote-id <i>remote-string</i> [circuit-id <i>circuit-string</i>]
Mode	DHCP Class Config

class (DHCP Pool Config)

M4250

M4350

This command binds an existing DHCP class to a DHCP pool. You can define an IP address range as part of the class.

When you define a class in DHCP Pool Config mode, the CLI enters the DHCP Pool Class Config mode. (To let the CLI enter the DHCP Pool Config mode, from Global Config mode, enter the **ip dhcp pool** *name* command.)

Default	None
Format	<i>class name</i>
Mode	DHCP Pool Config

Command example:

```
(NETGEAR Switch) (Config)#ip dhcp pool POOLNAME1
(NETGEAR Switch) (Config-dhcp-pool)#class CLASS1
(NETGEAR Switch) (Config-dhcp-pool-class)#
```

no class (DHCP Pool Config)

This command removes a class from a DHCP pool.

Format	<i>no class name</i>
Mode	DHCP Pool Config

address range (DHCP Pool Class Config)

M4250

M4350

This command configures the address range for a class in a DHCP pool. The address range of individual classes must be from the same subnet as the DHCP pool part from which the classes are defined.

All DHCP classes under a pool must have a unique IP address range. This ensures that each DHCP client receives a unique IP address from a pool.

You can also configure only the start address, which implies a single IP address, that is, the start and the end addresses are the same.

Default	None
Format	<i>address range ip-address-start [ip-address-end]</i>
Mode	DHCP Pool Class Config

Command example:

```
(NETGEAR Switch) (Config)#ip dhcp pool POOLNAME1
(NETGEAR Switch) (Config-dhcp-pool)#network 1.2.3.0 24
(NETGEAR Switch) (Config-dhcp-pool)#class CLASS1
(NETGEAR Switch) (Config-dhcp-pool-class)#address range 1.2.3.4 1.2.3.10
```


no address range (DHCP Pool Class Config)

This command removes the address range for a class in a DHCP pool.

Format	no address range

Mode	DHCP Pool Class Config

bootfile (DHCP Pool Class Config)

M4250

M4350

The command specifies the name of the default boot image for a class in DHCP pool. The *filename* specifies the boot image file.

Format	bootfile filename

Mode	DHCP Pool Class Config

no bootfile (DHCP Pool Class Config)

This command deletes the boot image name for a class in DHCP pool.

Format	no bootfile

Mode	DHCP Pool Class Config

deny lease (DHCP Pool Class Config)

M4250

M4350

This command denies the lease to a client based on a DHCP class and its configuration within a pool. You first must specify the client (or clients) using the **network** command in Config DHCP Pool mode..

Format	deny lease

Mode	DHCP Pool Class Config

Command example:

```
(localhost) (Config) #ip dhcp pool POOLNAME1
(localhost) (Config-dhcp-pool) #network 192.168.10.0 24
(localhost) (Config-dhcp-pool) #class CLASS1
(localhost) (Config-dhcp-pool-class) #deny lease
```

no deny lease (DHCP Pool Class Config)

This command removes the lease denial to a client based on a DHCP class and its configuration within a pool. You first must specify the client (or clients) using the **network** command in Config DHCP Pool mode..

Format	no deny lease

Mode	DHCP Pool Class Config

clear ip dhcp binding

M4250

M4350

This command deletes an automatic address binding from the DHCP server database. If * (the asterisk character) is specified, the bindings corresponding to all the addresses are deleted.

If you use the *ip-address* argument to specify an IP address made up of four decimal bytes ranging from 0 to 255, the bindings corresponding to the IP address are deleted. (IP address 0.0.0.0 is invalid.)

If you use the **pool** keyword and the associated *name* argument, the bindings for the specified pool are deleted.

Format	clear ip dhcp binding { * <i>ip-address</i> pool }

Mode	Privileged EXEC

clear ip dhcp server statistics

M4250

M4350

This command clears DHCP server statistics counters.

Format	clear ip dhcp server statistics

Mode	Privileged EXEC

clear ip dhcp conflict

M4250

M4350

The command is used to clear an address conflict from the DHCP server database. The server detects conflicts using a ping. If you use the * (asterisk) character as the address parameter, the DHCP server clears all conflicts.

Default	none
Format	clear ip dhcp conflict { <i>ip-address</i> *}
Mode	Privileged EXEC

show ip dhcp binding

M4250

M4350

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Format	show ip dhcp binding [<i>ip-address</i>]
Modes	Privileged EXEC User EXEC

Term	Definition
IP address	The IP address of the client.
Hardware Address	The MAC Address or the client identifier.
Lease expiration	The lease expiration time of the IP address assigned to the client.
Type	The manner in which IP address was assigned to the client.

show ip dhcp global configuration

M4250

M4350

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Format	show ip dhcp global configuration
Modes	Privileged EXEC User EXEC

Term	Definition
Service DHCP	The field to display the status of dhcp protocol.
Number of Ping Packets	The maximum number of Ping Packets that will be sent to verify that an ip address id not already assigned.
Conflict Logging	Shows whether conflict logging is enabled or disabled.
BootP Automatic	Shows whether BootP for dynamic pools is enabled or disabled.

show ip dhcp pool configuration

M4250

M4350

This command displays pool configuration. If **a11** is specified, configuration for all the pools is displayed.

Format	<code>show ip dhcp pool configuration {name all}</code>
Modes	Privileged EXEC User EXEC

Field	Definition
Pool Name	The name of the configured pool.
Pool Type	The pool type.
Lease Time	The lease expiration time of the IP address assigned to the client.
DNS Servers	The list of DNS servers available to the DHCP client.
Default Routers	The list of the default routers available to the DHCP client

The following additional field is displayed for Dynamic pool type.

Field	Definition
Network	The network number and the mask for the DHCP address pool.

The following additional fields are displayed for Manual pool type.

Field	Definition
Client Name	The name of a DHCP client.
Client Identifier	The unique identifier of a DHCP client.
Hardware Address	The hardware address of a DHCP client.

Field	Definition
Hardware Address Type	The protocol of the hardware platform.
Host	The IP address and the mask for a manual binding to a DHCP client.

show ip dhcp server statistics

M4250

M4350

This command displays DHCP server statistics.

Format	show ip dhcp server statistics
Modes	Privileged EXEC User EXEC

Field	Definition
Total Active Bindings	The number of IP addresses that are mapped to the MAC addresses of hosts that are found in the DHCP database.
Expired Bindings	The number of expired leases.
Malformed Bindings	The number of truncated or corrupted messages that were received by the DHCP server.
DHCP DISCOVER packets discarded	The number of DHCPDISCOVER messages that were discarded.
DHCP DISCOVER packets denied lease	The number of DHCPDISCOVER messages that were denied a lease.

Message Received.

Message	Definition
DHCP DISCOVER	The number of DHCPDISCOVER messages the server has received.
DHCP REQUEST	The number of DHCPREQUEST messages the server has received.
DHCP DECLINE	The number of DHCPDECLINE messages the server has received.
DHCP RELEASE	The number of DHCPRELEASE messages the server has received.
DHCP INFORM	The number of DHCPINFORM messages the server has received.

Message Sent.

Message	Definition
DHCP OFFER	The number of DHCPOFFER messages the server sent.
DHCP ACK	The number of DHCPACK messages the server sent.
DHCP NACK	The number of DHCPNACK messages the server sent.

show ip dhcp class configuration

This command displays the DHCP class configuration for all classes or for a specific class.

Format	<code>show ip dhcp class configuration {all name}</code>
Modes	Privileged EXEC

Field	Definition
Name	The DHCP class name.
Remote ID	The remote ID configured in the DHCP class.
Circuit ID	The circuit ID configured in the DHCP class.

Command example:

```
(NETGEAR Switch)#show ip dhcp class configuration Class1
```

```
Class: Class1
```

```
Remote ID                      Circuit ID
```

```
-----
```

```
COACH1                        1/0/13
```

show ip dhcp conflict

M4250

M4350

This command displays address conflicts logged by the DHCP Server. If no IP address is specified, all the conflicting addresses are displayed.

Format	<code>show ip dhcp conflict [ip-address]</code>
Modes	Privileged EXEC User EXEC

Term	Definition
IP address	The IP address of the host as recorded on the DHCP server.
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 found.

DNS Client Commands

These commands are used in the Domain Name System (DNS), an Internet directory service. DNS is how domain names are translated into IP addresses. When enabled, the DNS client provides a host name lookup service to other components.

ip domain lookup

M4250

M4350

Use this command to enable the DNS client.

Default	enabled
Format	ip domain lookup
Mode	Global Config

no ip domain lookup

Use this command to disable the DNS client.

Format	no ip domain lookup
Mode	Global Config

ip domain name

M4250

M4350

Use this command to define a default domain name that the switch uses to complete unqualified host names (names with a domain name). By default, no default domain name is configured in the system. *name* cannot be longer than 255 characters and cannot include an

initial period. *name* should be used only when the default domain name list, configured using the **ip domain list** command, is empty.

Default	none
Format	ip domain name <i>name</i>
Mode	Global Config

The CLI command **ip domain name yahoo.com** configures yahoo.com as a default domain name. For an unqualified hostname **xxx**, a DNS query is made to find the IP address corresponding to xxx.yahoo.com.

no ip domain name

Use this command to remove the default domain name configured using the **ip domain name** command.

Format	no ip domain name
Mode	Global Config

ip domain list

M4250

M4350

Use this command to define a list of default domain names to complete unqualified names. By default, the list is empty. Each name must be no more than 256 characters, and should not include an initial period. The default domain name, configured using the **ip domain name** command, is used only when the default domain name list is empty. A maximum of 32 names can be entered in to this list.

Default	none
Format	ip domain list <i>name</i>
Mode	Global Config

no ip domain list

Use this command to delete a name from a list.

Format	no ip domain list <i>name</i>
Mode	Global Config

ip name server

M4250

M4350

Use this command to configure the available name servers. Up to eight servers can be defined in one command or by using multiple commands. The parameter *server-address* is a valid IPv4 or IPv6 address of the server. The preference of the servers is determined by the order they were entered.

Format	<code>ip name-server server-address1 [server-address2...server-address8]</code>

Mode	Global Config

no ip name server

Use this command to remove a name server.

Format	<code>no ip name-server [server-address1...server-address8]</code>

Mode	Global Config

ip name source-interface

M4250

M4350

Use this command to specify the physical or logical interface to use as the DNS client (IP name) source interface (source IP address) for the DNS client management application. If configured, the address of source Interface is used for all DNS communications between the DNS server and the DNS client. The selected source-interface IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch. If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address. If the configured interface is down, the DNS client falls back to its default behavior.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>ip name source-interface {unit/slot/port loopback loopback-id serviceport vlan vlan-id}</code>

Mode	Global Config

no ip name source-interface

Use this command to reset the DNS source interface to the default settings.

Format	no ip name source-interface
Mode	Global Config

ip host

M4250

M4350

Use this command to define static host name-to-address mapping in the host cache. The parameter *name* is host name and *ipaddress* is the IP address of the host. The host name can include 1–255 alphanumeric characters, periods, hyphens, underscores, and non-consecutive spaces. Hostnames that include one or more space must be enclosed in quotation marks, for example “lab-pc 45”.

Default	none
Format	ip host <i>name ipaddress</i>
Mode	Global Config

no ip host

Use this command to remove the name-to-address mapping.

Format	no ip host <i>name</i>
Mode	Global Config

ipv6 host

M4250

M4350

Use this command to define static host name-to-IPv6 address mapping in the host cache. The parameter *name* is host name and *ipv6-address* is the IPv6 address of the host. The host name can include 1–255 alphanumeric characters, periods, hyphens, and spaces. Host names that include one or more space must be enclosed in quotation marks, for example “lab-pc 45”.

Default	none
Format	ipv6 host <i>name ipv6-address</i>
Mode	Global Config

no ipv6 host

Use this command to remove the static host name-to-IPv6 address mapping in the host cache.

Format	no ipv6 host <i>name</i>

Mode	Global Config

ip domain retry

M4250

M4350

Use this command to specify the number of times to retry sending Domain Name System (DNS) queries. The *number* argument indicates the number of times to retry sending a DNS query to the DNS server. This number is in the range from 0 to 100.

Default	2

Format	ip domain retry <i>number</i>

Mode	Global Config

no ip domain retry

Use this command to return to the default.

Format	no ip domain retry

Mode	Global Config

ip domain timeout

M4250

M4350

Use this command to specify the amount of time to wait for a response to a DNS query. The parameter *seconds* specifies the time, in seconds, to wait for a response to a DNS query. The parameter *seconds* ranges from 0 to 3600.

Default	3

Format	ip domain timeout <i>seconds</i>

Mode	Global Config

no ip domain timeout

Use this command to return to the default setting.

Format	no ip domain timeout

Mode	Global Config

clear host

M4250

M4350

Use this command to delete entries from the host name-to-address cache. This command clears the entries from the DNS cache maintained by the software. This command clears both IPv4 and IPv6 entries.

Format	clear host { <i>hostname</i> all}

Mode	Privileged EXEC

Field	Description
hostname	A particular host entry to remove. The parameter <i>hostname</i> ranges from 1-255 characters.
all	Removes all entries.

show hosts

M4250

M4350

Use this command to display the default domain name, a list of name server hosts, the static and the cached list of host names and addresses. The parameter *hostname* ranges from 1-255 characters. This command displays both IPv4 and IPv6 entries.

Format	show hosts [<i>hostname</i>]

Mode	Privileged Exec User EXEC

Field	Description
Host Name	Domain host name.
Default Domain	Default domain name.
Default Domain List	Default domain list.
Domain Name Lookup	DNS client enabled/disabled.

Fully Managed Switches M4250 and M4350 Series

Field	Description
Number of Retries	Number of time to retry sending Domain Name System (DNS) queries.
Retry Timeout Period	Amount of time to wait for a response to a DNS query.
Name Servers	Configured name servers.
DNS Client Source Interface	Shows the configured source interface (source IP address) used for a DNS client. The IP address of the selected interface is used as source IP for all communications with the server.

Command example:

```
(NETGEAR Switch) show hosts
Host name..... Device
Default domain..... gm.com
Default domain list..... yahoo.com, Stanford.edu, rediff.com
Domain Name lookup..... Enabled
Number of retries..... 5
Retry timeout period..... 1500
Name servers (Preference order)... 176.16.1.18 176.16.1.19
DNS Client Source Interface..... (not configured)
```

Configured host name-to-address mapping:

```
Host                               Addresses
-----
accounting.gm.com                  176.16.8.8

Host      Total    Elapsed    Type      Addresses
-----
www.stanford.edu      72          3          IP      171.64.14.203
```

IP Address Conflict Commands

The commands in this section help troubleshoot IP address conflicts.

ip address-conflict-detect run

M4250

M4350

This command triggers the switch to run active address conflict detection by sending gratuitous ARP packets for IPv4 addresses on the switch.

Format	ip address-conflict-detect run

Mode	Global Config

show ip address-conflict

M4250

M4350

This command displays the status information corresponding to the last detected address conflict.

Format	show ip address-conflict

Modes	Privileged EXEC

Term	Definition
Address Conflict Detection Status	Identifies whether the switch has detected an address conflict on any IP address.
Last Conflicting IP Address	The IP Address that was last detected as conflicting on any interface.
Last Conflicting MAC Address	The MAC Address of the conflicting host that was last detected on any interface.
Time Since Conflict Detected	The time in days, hours, minutes and seconds since the last address conflict was detected.

clear ip address-conflict-detect

M4250

M4350

This command clears the detected address conflict status information.

Format	clear ip address-conflict-detect

Modes	Privileged EXEC

Serviceability Packet Tracing Commands

These commands improve the capability to diagnose conditions that affect the switch.

**CAUTION:**

The output of debug commands can be long and may adversely affect system performance.

capture start

M4250

M4350

Use the **capture start** command to manually start capturing CPU packets for packet trace.

The packet capture operates in three modes:

- capture file
- remote capture
- capture line

The command is not persistent across a reboot cycle.

Format	capture start [all receive transmit]
Mode	Privileged EXEC
Parameter	Description
all	Capture all traffic.
receive	Capture only received traffic.
transmit	Capture only transmitted traffic.

capture stop

M4250

M4350

Use the **capture stop** command to manually stop capturing CPU packets for packet trace.

Format	capture stop
Mode	Privileged EXEC

capture {file | remote | line | usb}

M4250

M4350

Use this command to configure file capture options. The command is persistent across a reboot cycle.

Format	capture {file remote line usb}
Mode	Global Config
Parameter	Description
file	In the capture file mode, the captured packets are stored in a file on NVRAM. The maximum file size defaults to 524288 bytes. The switch can transfer the file to a TFTP server via TFTP, SFTP, SCP via CLI, and SNMP. The file is formatted in pcap format, is named cpuPktCapture.pcap, and can be examined using network analyzer tools such as Wireshark® or Ethereal®. Starting a file capture automatically terminates any remote capture sessions and line capturing. After the packet capture is activated, the capture proceeds until the capture file reaches its maximum size, or until the capture is stopped manually using the CLI command capture stop.
remote	In the remote capture mode, the captured packets are redirected in real time to an external PC running the Wireshark tool for Microsoft® Windows®. A packet capture server runs on the switch side and sends the captured packets via a TCP connection to the Wireshark tool. The remote capture can be enabled or disabled using the CLI. There should be a Windows PC with the Wireshark tool to display the captured file. When using the remote capture mode, the switch does not store any captured data locally on its file system. You can configure the IP port number for connecting Wireshark to the switch. The default port number is 2002. If a firewall is installed between the Wireshark PC and the switch, then these ports must be allowed to pass through the firewall. You must configure the firewall to allow the Wireshark PC to initiate TCP connections to the switch. If the client successfully connects to the switch, the CPU packets are sent to the client PC, then Wireshark receives the packets and displays them. This continues until the session is terminated by either end. Starting a remote capture session automatically terminates the file capture and line capturing.
line	In the capture line mode, the captured packets are saved into the RAM and can be displayed on the CLI. Starting a line capture automatically terminates any remote capture session and capturing into a file. There is a maximum 128 packets of maximum 128 bytes that can be captured and displayed in line mode.
usb	In the usb mode, the captured packets are stored in a file on USB device.

capture remote port

M4250**M4350**

Use this command to configure file capture options. The command is persistent across a reboot cycle. The *port-id* argument is a TCP port number from 1024– 49151.

Format	<code>capture remote port <i>port-id</i></code>

Mode	Global Config

capture file size

M4250**M4350**

Use this command to configure file capture options. The command is persistent across a reboot cycle. The *file-size* argument is the maximum size the PCAP file can reach, which is 2–512 KB.

Format	<code>capture file size <i>max file-size</i></code>

Mode	Global Config

capture line wrap

M4250**M4350**

This command enables wrapping of captured packets in line mode when the captured packets reaches full capacity.

Format	<code>capture line wrap</code>

Mode	Global Config

no capture line wrap

This command disables wrapping of captured packets and configures capture packet to stop when the captured packet capacity is full.

Format	<code>no capture line wrap</code>

Mode	Global Config

capture usb

M4250**M4350**

This command sets a file name on a USB device as the destination for the capture of CPU packets.

Format	<code>capture usb <i>file-name</i></code>

Mode	Global Config

show capture packets

M4250**M4350**

Use this command to display packets captured and saved to RAM. It is possible to capture and save into RAM, packets that are received or transmitted through the CPU. A maximum 128 packets can be saved into RAM per capturing session. A maximum 128 bytes per packet can be saved into the RAM. If a packet holds more than 128 bytes, only the first 128 bytes are saved; data more than 128 bytes is skipped and cannot be displayed in the CLI.

Capturing packets is stopped automatically when 128 packets are captured and have not yet been displayed during a capture session. Captured packets are not retained after a reload cycle.

Format	<code>show capture packets</code>

Mode	Privileged EXEC

debug aaa accounting

M4250**M4350**

This command is useful to debug accounting configuration and functionality in User Manager

Note: To display the debug trace, enable the `debug console` command.

Format	<code>debug aaa accounting</code>

Mode	Privileged EXEC

no debug aaa accounting

Use this command to turn off debugging of User Manager accounting functionality.

Format	no debug aaa accounting

Mode	Privileged EXEC

debug aaa authorization

M4250

M4350

Use this command to enable the tracing for AAA in User Manager. This is useful to debug authorization configuration and functionality in the User Manager. Each of the parameters are used to configure authorization debug flags.

Note: To display the debug trace, enable the debug console command.

Format	debug aaa authorization [commands exec]

Mode	Privileged EXEC

no debug aaa authorization

Use this command to turn off debugging of the User Manager authorization functionality.

Format	no debug aaa authorization

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #debug aaa authorization
Tacacs authorization receive packet tracing enabled.
```

```
(NETGEAR Switch) #debug tacacs authorization packet transmit
authorization tracing enabled.
```

```
(NETGEAR Switch) #no debug aaa authorization
AAA authorization tracing enabled
```

```
(NETGEAR Switch) #
```

debug aaa coa

M4250

M4350

This command is useful to debug accounting DAS control messages in User Manager

Note: To display the debug trace, enable the debug console command.

Format	debug aaa coa

Mode	Privileged EXEC

no debug aaa coa

Use this command to turn off debugging of User Manager DAS control messages.

Format	no debug aaa coa

Mode	Privileged EXEC

debug aaa pod

M4250

M4350

This command is useful to debug accounting DAS packets in User Manager

Note: To display the debug trace, enable the debug console command.

Format	debug aaa pod

Mode	Privileged EXEC

no debug aaa pod

Use this command to turn off debugging of User Manager DAS packets.

Format	no debug aaa pod

Mode	Privileged EXEC

debug arp

M4250**M4350**

Use this command to enable ARP debug protocol messages.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug arp
Mode	Privileged EXEC

no debug arp

Use this command to disable ARP debug protocol messages.

Format	no debug arp
Mode	Privileged EXEC

debug authentication

M4250**M4350**

This command displays either the debug trace for either a single event or all events for an interface.

Note: To display the debug trace, enable the debug console command.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Default	none
Format	debug authentication packet {all event} <i>unit/slot/port</i>
Mode	Privileged EXEC

debug auto-voip

M4250

M4350

Use this command to enable Auto VoIP debug messages. Use the optional parameters to trace H323, SCCP, or SIP packets respectively.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug auto-voip [H323 SCCP SIP]
Mode	Privileged EXEC

no debug auto-voip

Use this command to disable Auto VoIP debug messages.

Format	no debug auto-voip
Mode	Privileged EXEC

debug auto-vlan

M4250

M4350

Use this command to enable debug the Auto-VLAN feature.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug auto-vlan
Mode	Privileged EXEC

no debug auto-vlan

Use this command to disable Auto-VLAN debug messages.

Format	no debug auto-vlan
Mode	Privileged EXEC

debug clear

M4250

M4350

This command disables all previously enabled “debug” traces.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug clear
Mode	Privileged EXEC

debug console

M4250

M4350

This command enables the display of “debug” trace output on the login session in which it is executed. Debug console display must be enabled in order to view any trace output. The output of debug trace commands will appear on all login sessions for which debug console has been enabled. The configuration of this command remains in effect for the life of the login session. The effect of this command is not persistent across resets.

Default	disabled
Format	debug console
Mode	Privileged EXEC

no debug console

This command disables the display of “debug” trace output on the login session in which it is executed.

Format	no debug console
Mode	Privileged EXEC

debug crashlog (M4250 series switch)

M4250

Use this command on an M4250 series switch to view information contained in the crash log file that the system maintains when it experiences an unexpected reset. The crash log file contains the following information:

- Call stack information in both primitive and verbose forms
- Log Status

- Buffered logging
- Event logging
- Persistent logging
- System Information (output of sysapiMbufDump)
- Message Queue Debug Information
- Memory Debug Information
- Memory Debug Status
- OS Information (output of osapiShowTasks)
- process information (meminfo, cpuinfo, interrupts, version and net/sockstat)

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug crashlog {proc verbose deleteall <i>crashlog-number</i> [export url] {data <i>crashlog-number</i> [upgrade url export url component-id item-number additional-parameter]}}
Mode	Privileged EXEC

Parameter	Description
proc	View the application process crashlog.
verbose	Enable the verbose crashlog.
deleteall	Delete all crash log files on the system.
crashlog-number	Specifies the file number to view. The system maintains up to four copies, and the valid range is 1–4.
export url	To upload the crash log (or crash dump) to a TFTP server, use the export keyword and specify the required TFTP server information.
data	Crash log data recorder.
crashdump-number	Specifies the crash dump number to view. The valid range is 0–2.
upgrade url	To download a crash dump to the switch, use the upgrade keyword and specify the required TFTP server information.
component-id	The ID of the component that caused the crash.
item-number	The item number.
additional-parameter	Additional parameters to include. You can include up to two parameters.

debug crashlog (M4350 series switch)

M4350

Use this command on an M4350 series switch to view information contained in the crash log file that the system maintains when it experiences an unexpected reset. The crash log file contains the following information:

- Call stack information in both primitive and verbose forms
- Log Status
- Buffered logging
- Event logging
- Persistent logging
- System Information (output of sysapiMbufDump)
- Message Queue Debug Information
- Memory Debug Information
- Memory Debug Status
- OS Information (output of osapiShowTasks)
- process information (meminfo, cpuinfo, interrupts, version and net/sockstat)

Note: To display the debug trace, enable the [debug console](#) command.

Default	disabled
Format	<code>debug crashlog {proc verbose deleteall crashlog-number [[export url] [slot slot-number]] {data crashlog-number [upgrade url export url [slot slot-number] component-id item-number additional-parameter [slot slot-number]]}}</code>
Mode	Privileged EXEC
Parameter	Description
proc	View the application process crashlog.
verbose	Enable the verbose crashlog.
deleteall	Delete all crash log files on the system.
crashlog-number	Specifies the file number to view. The system maintains up to four copies, and the valid range is 1–4.
export url	To upload the crash log (or crash dump) to a TFTP server, use the export keyword and specify the required TFTP server information.
slot	The slot or unit number for the unit on which the crashlog is located.
data	Crash log data recorder.
crashdump-number	Specifies the crash dump number to view. The valid range is 0–2.

Parameter	Description
<code>upgrade url</code>	To download a crash dump to the switch, use the upgrade keyword and specify the required TFTP server information.
<code>component-id</code>	The ID of the component that caused the crash.
<code>item-number</code>	The item number.
<code>additional-parameter</code>	Additional parameters to include. You can include up to two parameters.

debug debug-config

M4250

M4350

Use this command to upload (export) or download (upgrade) the debug-config.ini file. The debug-config.ini file executes CLI commands on specific predefined events. The debug config file is created manually and downloaded to the switch.

Note: To display the debug trace, enable the `debug console` command.

Default	disabled
Format	<code>debug debug-config {export url upgrade url}</code>
Mode	Privileged EXEC

debug dhcp packet

M4250

M4350

This command displays “debug” information about DHCPv4 client activities and traces DHCPv4 packets to and from the local DHCPv4 client.

Note: To display the debug trace, enable the `debug console` command.

Default	disabled
Format	<code>debug dhcp packet [transmit receive]</code>
Mode	Privileged EXEC

no debug dhcp packet

This command disables the display of “debug” trace output for DHCPv4 client activity.

Format	<code>no debug dhcp packet [transmit receive]</code>
Mode	Privileged EXEC

debug dhcp server packet

M4250

M4350

This command displays “debug” information about DHCPv4 server activities and traces DHCPv4 packets to and from the local DHCPv4 client.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug dhcp server packet
Mode	Privileged EXEC

no debug dhcp server packet

This command disables the display of “debug” trace output for DHCPv4 server activity.

Format	no debug dhcp server packet
Mode	Privileged EXEC

debug dot1x packet

M4250

M4350

Use this command to enable dot1x packet debug trace.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug dot1x [transmit receive]
Mode	Privileged EXEC

no debug dot1x packet

Use this command to disable dot1x packet debug trace.

Format	no debug dot1x [transmit receive]
Mode	Privileged EXEC

debug drop-counters start

M4250

M4350

This command starts collecting egress or ingress packet drop counters. Use the **debug drop-counters stop** command to stop the collection of packet drop counters.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Use the optional L2, L3, or L2L3 keyword to limit the packet drop collection to Layer 2 level (L2), Layer 3 level (L3) or both Layer 2 and 3 level (L2L3) packet drops.

Default	disabled
Format	debug drop-counters {egress ingress} interface <i>unit/slot/port</i> start [L2 L2L3 L3]
Mode	Privileged EXEC

debug drop-counters stop

M4250

M4350

This command stops collecting packet drop counters.

Default	disabled
Format	debug drop-counters stop
Mode	Privileged EXEC

debug drop-counters show

M4250

M4350

This command displays collected packet drop counters.

Format	debug drop-counters show
Mode	Privileged EXEC

debug igmpsnooping packet

M4250**M4350**

This command enables tracing of IGMP snooping packets received and transmitted by the switch.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug igmpsnooping packet [transmit receive]
Mode	Privileged EXEC

no debug igmpsnooping packet

This command disables tracing of IGMP snooping packets.

Format	no debug igmpsnooping packet
Mode	Privileged EXEC

debug igmpsnooping packet transmit

M4250**M4350**

This command enables tracing of IGMP snooping packets transmitted by the switch. Snooping must be enabled on the device and the interface in order to monitor packets for a particular interface.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug igmpsnooping packet transmit
Mode	Privileged EXEC

The following sample shows the output of the trace message.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMP Snooping[185429992]: igmp_snooping_debug.c(116)
908 % Pkt TX - Intf: 1/0/20(20), Vlan_Id:1 Src_Mac: 00:03:0e:00:00:00 Dest_Mac:
01:00:5e:00:00:01 Src_IP: 9.1.1.1 Dest_IP: 225.0.0.1 Type: V2_Membership_Report Group:
225.0.0.1
```

The following parameters are displayed in the trace message.

Parameter	Definition
TX	A packet transmitted by the device.
Intf	The interface that the packet left from. Format used is unit/port (internal interface number).
Src_Mac	Source MAC address of the packet.
Dest_Mac	Destination multicast MAC address of the packet.
Src_IP	The source IP address in the IP header in the packet.
Dest_IP	The destination multicast IP address in the packet.
Type	The type of IGMP packet. Type can be one of the following: • Membership Query. GMP Membership Query • V1_Membership_Report. IGMP Version 1 Membership Report • V2_Membership_Report. IGMP Version 2 Membership Report • V3_Membership_Report. IGMP Version 3 Membership Report • V2_Leave_Group. IGMP Version 2 Leave Group
Group	Multicast group address in the IGMP header.

no debug igmpsnooping transmit

This command disables tracing of transmitted IGMP snooping packets.

Format	no debug igmpsnooping transmit
Mode	Privileged EXEC

debug igmpsnooping packet receive

M4250

M4350

This command enables tracing of IGMP snooping packets received by the switch. Snooping must be enabled on the device and the interface in order to monitor packets for a particular interface.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug igmpsnooping packet receive
Mode	Privileged EXEC

The following sample shows the output of the trace message.

Fully Managed Switches M4250 and M4350 Series

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMP Snooping[185429992]: igmp_snooping_debug.c(116)
908 % Pkt RX - Intf: 1/0/20(20), Vlan_Id:1 Src_Mac: 00:03:0e:00:00:10 Dest_Mac:
01:00:5e:00:00:05 Src_IP: 11.1.1.1 Dest_IP: 225.0.0.5 Type: Membership_Query Group:
225.0.0.5
```

The following parameters are displayed in the trace message.

Parameter	Definition
RX	A packet received by the device.
Intf	The interface that the packet went out on.
Src_Mac	Source MAC address of the packet.
Dest_Mac	Destination multicast MAC address of the packet.
Src_IP	The source IP address in the ip header in the packet.
Dest_IP	The destination multicast ip address in the packet.
Type	The type of IGMP packet. Type can be one of the following: • Membership_Query. IGMP Membership Query • V1_Membership_Report. IGMP Version 1 Membership Report • V2_Membership_Report. IGMP Version 2 Membership Report • V3_Membership_Report. IGMP Version 3 Membership Report • V2_Leave_Group. IGMP Version 2 Leave Group
Group	Multicast group address in the IGMP header.

no debug igmpsnooping receive

This command disables tracing of received IGMP snooping packets.

Format	no debug igmpsnooping receive
Mode	Privileged EXEC

debug ip acl

M4250

M4350

Use this command to enable debug of IP Protocol packets matching the ACL criteria.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug ip acl <i>number</i>
Mode	Privileged EXEC

no debug ip acl

Use this command to disable debug of IP Protocol packets matching the ACL criteria.

Format	no debug ip acl number
Mode	Privileged EXEC

debug ip dvmrp packet

M4350

Use this command to trace DVMRP packet reception and transmission. The **receive** keyword traces only received DVMRP packets and **transmit** keyword traces only transmitted DVMRP packets. When neither keyword is used in the command, then all DVMRP packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug ip dvmrp packet [receive transmit]
Mode	Privileged EXEC

no debug ip dvmrp packet

Use this command to disable debug tracing of DVMRP packet reception and transmission.

Format	no debug ip dvmrp packet [receive transmit]
Mode	Privileged EXEC

debug ip igmp packet

M4250

M4350

Use this command to trace IGMP packet reception and transmission. The **receive** keyword traces only received IGMP packets and the **transmit** keyword traces only transmitted IGMP packets. When neither keyword is used in the command, then all IGMP packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Note: To display the debug trace, enable the debug console command.

Default	disabled

Format	debug ip igmp packet [receive transmit]

Mode	Privileged EXEC

no debug ip igmp packet

Use this command to disable debug tracing of IGMP packet reception and transmission.

Format	no debug ip igmp packet [receive transmit]

Mode	Privileged EXEC

debug ip mcache packet

M4250

M4350

Use this command for tracing MDATA packet reception and transmission. The **receive** keyword traces only received MDATA packets and the **transmit** keyword traces only transmitted MDATA packets. When neither keyword is used in the command, then all data packet traces are dumped. Vital information such as source address, destination address, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Note: To display the debug trace, enable the [debug console](#) command.

Default	disabled

Format	debug ip mcache packet [receive transmit]

Mode	Privileged EXEC

no debug ip mcache packet

Use this command to disable debug tracing of MDATA packet reception and transmission.

Format	no debug ip mcache packet [receive transmit]

Mode	Privileged EXEC

debug ip pimdm packet

M4250

M4350

Use this command to trace PIMDM packet reception and transmission. The **receive** keyword traces only received PIMDM packets and the **transmit** keyword traces only

transmitted PIMDM packets. When neither keyword is used in the command, then all PIMDM packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Note: To display the debug trace, enable the [debug console](#) command.

Default	disabled
Format	debug ip pimdm packet [receive transmit]
Mode	Privileged EXEC

no debug ip pimdm packet

Use this command to disable debug tracing of PIMDM packet reception and transmission.

Format	no debug ip pimdm packet [receive transmit]
Mode	Privileged EXEC

debug ip pimsm packet

M4250

M4350

Use this command to trace PIMSM packet reception and transmission. The **receive** keyword traces only received PIMSM packets and the **transmit** keyword traces only transmitted PIMSM packets. When neither keyword is used in the command, then all PIMSM packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Note: To display the debug trace, enable the [debug console](#) command.

Default	disabled
Format	debug ip pimsm packet [receive transmit]
Mode	Privileged EXEC

no debug ip pimsm packet

Use this command to disable debug tracing of PIMSM packet reception and transmission.

Format	no debug ip pimsm packet [receive transmit]
Mode	Privileged EXEC

debug ipv6 dhcp

M4250

M4350

This command displays “debug” information about DHCPv6 client, relay, or server activities and traces DHCPv6 packets to, from, or both to and from the local DHCPv6 client, relay, or server.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug ipv6 dhcp {client relay server} [receive transmit]
Mode	Privileged EXEC

no debug ipv6 dhcp

This command disables the display of “debug” trace output for DHCPv6 client, relay, or server activities.

Format	no debug ipv6 dhcp {client relay server} [receive transmit]
Mode	Privileged EXEC

debug ipv6 mcache packet

M4250

M4350

Use this command for tracing MDATAv6 packet reception and transmission. The **receive** keyword traces only received MDATAv6 packets and the **transmit** keyword traces only transmitted MDATAv6 packets. When neither keyword is used in the command, then all data packet traces are dumped. Vital information such as source address, destination address, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug ipv6 mcache packet [receive transmit]
Mode	Privileged EXEC

no debug ipv6 mcache packet

Use this command to disable debug tracing of MDATAv6 packet reception and transmission.

Format	no debug ipv6 mcache packet [receive transmit]
Mode	Privileged EXEC

debug ipv6 mld packet

M4250

M4350

Use this command to trace MLDv6 packet reception and transmission. The **receive** keyword traces only received MLDv6 packets and the **transmit** keyword traces only transmitted MLDv6 packets. When neither keyword is used in the command, then all MLDv6 packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Note: To display the debug trace, enable the [debug console](#) command.

Default	disabled
Format	debug ipv6 mld packet [receive transmit]
Mode	Privileged EXEC

no debug ipv6 mld packet

Use this command to disable debug tracing of MLDv6 packet reception and transmission.

Format	no debug ipv6 mld packet [receive transmit]
Mode	Privileged EXEC

debug ipv6 pimdm packet

M4250

M4350

Use this command to trace PIMDMv6 packet reception and transmission. The **receive** keyword traces only received PIMDMv6 packets and the **transmit** keyword traces only transmitted PIMDMv6 packets. If neither keyword is used in the command, all PIMDMv6 packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Note: To display the debug trace, enable the [debug console](#) command.

Default	disabled
Format	debug ipv6 pimdm packet [receive transmit]
Mode	Privileged EXEC

no debug ipv6 pimdm packet

Use this command to disable debug tracing of PIMDMv6 packet reception and transmission.

Format	no debug ipv6 pimdm packet [receive transmit]
Mode	Privileged EXEC

debug ipv6 pimsm packet

M4250

M4350

Use this command to trace PIMSMv6 packet reception and transmission. The **receive** keyword traces only received PIMSMv6 packets and the **transmit** keyword traces only transmitted PIMSMv6 packets. If neither keyword is used in the command, all PIMSMv6 packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Note: To display the debug trace, enable the [debug console](#) command.

Default	disabled
Format	debug ipv6 pimsm packet [receive transmit]
Mode	Privileged EXEC

no debug ipv6 pimsm packet

Use this command to disable debug tracing of PIMSMv6 packet reception and transmission.

Format	no debug ipv6 pimsm packet [receive transmit]
Mode	Privileged EXEC

debug lacp packet

M4250

M4350

This command enables tracing of LACP packets received and transmitted by the switch.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug lacp packet
Mode	Privileged EXEC

The following sample shows the output of the trace message.

```
<15> JAN 01 14:04:51 10.254.24.31-1 DOT3AD[183697744]: dot3ad_debug.c(385) 58 %%
Pkt TX - Intf: 1/0/1(1), Type: LACP, Sys: 00:11:88:14:62:e1, State: 0x47, Key: 0x36
```

no debug lacp packet

This command disables tracing of LACP packets.

Format	no debug lacp packet
Mode	Privileged EXEC

debug lldp packet

M4250

M4350

Use this command to enable debug tracing for LLDP packets. The optional **receive** keyword traces only received LLDP packets and the optional **transmit** keyword traces only transmitted LLDP packets.

Default	Disabled
Format	debug lldp packet [receive transmit]
Mode	Privileged Exec

no debug lldp packet

Use this command to disable debug tracing for LLDP packets.

Format	no debug lldp packet [receive transmit]
Mode	Privileged Exec

debug mldsnooping packet

M4250**M4350**

Use this command to trace MLD snooping packet reception and transmission. The **receive** keyword traces only received MLD packets and the **transmit** keyword traces only transmitted MLD snooping packets. When neither keyword is used in the command, then all MLD snooping packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug mldsnooping packet [receive transmit]
Mode	Privileged EXEC

no debug mldsnooping packet

Use this command to disable debug tracing of MLD snooping packet reception and transmission.

Format	no debug mldsnooping packet [receive transmit]
Mode	Privileged EXEC

debug ping packet

M4250**M4350**

This command enables tracing of ICMP echo requests and responses. The command traces pings on the network port/ service port for switching packages. For routing packages, pings are traced on the routing ports as well.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug ping packet
Mode	Privileged EXEC

The following sample shows the output of the trace message.

```
<15> JAN 01 00:21:22 192.168.17.29-1 SIM[181040176]: sim_debug.c(128) 20 % Pkt TX - Intf:
1/0/1(1),
SRC_IP:10.50.50.2, DEST_IP:10.50.50.1, Type:ECHO_REQUEST
```

```
<15> JAN 01 00:21:22 192.168.17.29-1 SIM[182813968]: sim_debug.c(82) 21 % Pkt RX - Intf:
1/0/1(1), S
RC_IP:10.50.50.1, DEST_IP:10.50.50.2, Type:ECHO_REPLY
```

The following parameters are displayed in the trace message.

Parameter	Definition
TX/RX	TX refers to a packet transmitted by the device. RX refers to packets received by the device.
Intf	The interface that the packet came in or went out on.
SRC_IP	The source IP address in the IP header in the packet.
DEST_IP	The destination IP address in the IP header in the packet.
Type	Type determines whether or not the ICMP message is a REQUEST or a RESPONSE.

no debug ping packet

This command disables tracing of ICMP echo requests and responses.

Format	no debug ping packet
Mode	Privileged EXEC

debug ospf packet

M4350

This command enables tracing of OSPF packets received and transmitted by the switch.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug ospf packet
Mode	Privileged EXEC

Command example:

The following samples show the output of the trace message.

```
<15> JAN 02 11:03:31 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(297) 25430 % Pkt RX -
Intf:2/0/48 Src
Ip:192.168.50.2 DestIp:224.0.0.5 AreaId:0.0.0.0 Type:HELLO NetMask:255.255.255.0 D
esigRouter:0.0.0.0 Backup:0.0.0.0

<15> JAN 02 11:03:35 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25431 % Pkt TX -
Intf:2/0/48 Src
```


Fully Managed Switches M4250 and M4350 Series

```
Ip:10.50.50.1 DestIp:192.168.50.2 AreaId:0.0.0.0 Type:DB_DSCR Mtu:1500 Options:E  
Flags: I/M/MS Seq:126166
```

```
<15> JAN 02 11:03:36 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(297) 25434 % Pkt RX -  
Intf:2/0/48 Src  
Ip:192.168.50.2 DestIp:192.168.50.1 AreaId:0.0.0.0 Type:LS_REQ Length: 1500
```

```
<15> JAN 02 11:03:36 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25435 % Pkt TX -  
Intf:2/0/48 Src  
Ip:10.50.50.1 DestIp:192.168.50.2 AreaId:0.0.0.0 Type:LS_UPD Length: 1500
```

```
<15> JAN 02 11:03:37 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25441 % Pkt TX -  
Intf:2/0/48 Src  
Ip:10.50.50.1 DestIp:224.0.0.6 AreaId:0.0.0.0 Type:LS_ACK Length: 1500
```

The following parameters are displayed in the trace message.

Parameter	Definition
TX/RX	TX refers to a packet transmitted by the device. RX refers to packets received by the device.
Intf	The interface that the packet came in or went out on. Format used is unit/slot/port (internal interface number).
SrcIp	The source IP address in the IP header of the packet.
DestIp	The destination IP address in the IP header of the packet.
AreaId	The area ID in the OSPF header of the packet.
Type	Could be one of the following: • HELLO. Hello packet • DB_DSCR. Database descriptor • LS_REQ. LS Request • LS_UPD. LS Update • LS_ACK. LS Acknowledge

The remaining fields in the trace are specific to the type of OSPF packet.

HELLO packet field definitions.

Parameter	Definition
Netmask	The netmask in the hello packet.
DesignRouter	Designated Router IP address.
Backup	Backup router IP address.

DB_DSCR packet field definitions.

Field	Definition
MTU	MTU
Options	Options in the OSPF packet.
Flags	Could be one or more of the following: • I. Init • M. More • MS. Master/Slave
Seq	Sequence Number of the DD packet.

LS_REQ packet field definitions.

Field	Definition
Length	Length of packet

LS_UPD packet field definitions.

Field	Definition
Length	Length of packet

LS_ACK packet field definitions.

Field	Definition
Length	Length of packet

no debug ospf packet

This command disables tracing of OSPF packets.

Format	no debug ospf packet
Mode	Privileged EXEC

debug rip packet

M4250

M4350

This command turns on tracing of RIP requests and responses. The output is directed to the log file.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug rip packet
Mode	Privileged EXEC

The following sample shows the output of the trace message.

```
<15> JAN 01 00:35:15 192.168.17.29-1 RIP[181783160]: rip_map_debug.c(96) 775 %
Pkt RX on Intf: 1/0/1(1), Src_IP:43.1.1.1 Dest_IP:43.1.1.2
Rip_Version: RIPv2 Packet_Type:RIP_RESPONSE
ROUTE 1): Network: 10.1.1.0 Mask: 255.255.255.0 Metric: 1
ROUTE 2): Network: 40.1.0.0 Mask: 255.255.0.0 Metric: 1
ROUTE 3): Network: 10.50.50.0 Mask: 255.255.255.0 Metric: 1
ROUTE 4): Network: 41.1.0.0 Mask: 255.255.0.0 Metric: 1
ROUTE 5): Network:42.0.0.0 Mask:255.0.0.0 Metric:1
Another 6 routes present in packet not displayed.
```

The following parameters are displayed in the trace message.

Parameter	Definition
TX/RX	TX refers to a packet transmitted by the device. RX refers to packets received by the device.
Intf	The interface that the packet came in or went out on.
Src_IP	The source IP address in the IP header of the packet.
Dest_IP	The destination IP address in the IP header of the packet.
Rip_Version	RIP version used: RIPv1 or RIPv2.
Packet_Type	Type of RIP packet: RIP_REQUEST or RIP_RESPONSE.
Routes	Up to 5 routes in the packet are displayed in the following format: • Network. a.b.c.d • Mask. a.b.c.d • Next Hop. a.b.c.d • Metric. a The next hop is only displayed if it is different from 0.0.0.0. For RIPv1 packets, Mask is always 0.0.0.0.
Number of routes not printed	Only the first five routes present in the packet are included in the trace. There is another notification of the number of additional routes present in the packet that were not included in the trace.

no debug rip packet

This command disables tracing of RIP requests and responses.

Format	no debug rip packet
Mode	Privileged EXEC

debug sflow packet

M4250

M4350

Use this command to enable sFlow debug packet trace.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug sflow packet
Mode	Privileged EXEC

no debug sflow packet

Use this command to disable sFlow debug packet trace.

Format	no debug sflow packet
Mode	Privileged EXEC

debug spanning-tree bpdu

M4250

M4350

This command enables tracing of spanning tree BPDUs received and transmitted by the switch.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug spanning-tree bpdu
Mode	Privileged EXEC

no debug spanning-tree bpdu

This command disables tracing of spanning tree BPDUs.

Format	no debug spanning-tree bpdu

Mode	Privileged EXEC

debug spanning-tree bpdu receive

M4250

M4350

This command enables tracing of spanning tree BPDUs received by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets for a particular interface.

Note: To display the debug trace, enable the debug console command.

Default	disabled

Format	debug spanning-tree bpdu receive

Mode	Privileged EXEC

The following sample shows the output of the trace message.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 % Pkt RX
- Intf: 1/0/9(9), Source_Mac: 00:11:88:4e:c2:10 Version: 3, Root Mac: 00:11:88:4e:c2:00,
Root Priority: 0x8000 Path Cost: 0
```

The following parameters are displayed in the trace message.

Parameter	Definition
RX	A packet received by the device.
Intf	The interface that the packet came in on.
Source_Mac	Source MAC address of the packet.
Version	Spanning tree protocol version (0-3). 0 refers to STP, 2 RSTP and 3 MSTP.
Root_Mac	MAC address of the CIST root bridge.
Root_Priority	Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

no debug spanning-tree bpdu receive

This command disables tracing of received spanning tree BPDUs.

Format	no debug spanning-tree bpdu receive
Mode	Privileged EXEC

debug spanning-tree bpdu transmit

M4250

M4350

This command enables tracing of spanning tree BPDUs transmitted by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets on a particular interface.

Note: To display the debug trace, enable the debug console command.

Default	disabled
Format	debug spanning-tree bpdu transmit
Mode	Privileged EXEC

The following sample shows the output of the trace message.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 % Pkt TX
- Intf: 1/0/7(7), Source_Mac: 00:11:88:4e:c2:00 Version: 3, Root_Mac: 00:11:88:4e:c2:00,
Root_Priority: 0x8000 Path_Cost: 0
```

The following parameters are displayed in the trace message.

Parameter	Definition
TX	A packet transmitted by the device.
Intf	The interface that the packet went out on.
Source_Mac	Source MAC address of the packet.
Version	Spanning tree protocol version (0-3). 0 refers to STP, 2 RSTP and 3 MSTP.
Root_Mac	MAC address of the CIST root bridge.
Root_Priority	Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

no debug spanning-tree bpdu transmit

This command disables tracing of transmitted spanning tree BPDUs.

Format	no debug spanning-tree bpdu transmit

Mode	Privileged EXEC

debug tacacs

M4250

M4350

This command enables TACACS+ debugging.

Note: To display the debug trace, enable the debug console command.

Format	debug tacacs {packet accounting authentication authorization}

Mode	Global Config

Parameter	Description
packet	Turn on TACACS+ packet debugs for received and transmitted packets.
accounting	Turn on TACACS+ accounting debugging.
authentication	Turn on TACACS+ authentication debugging.
authorization	Turn on TACACS+ authorization debugging.

no debug tacacs

This command disables TACACS+ debugging.

Format	no debug tacacs {packet accounting authentication authorization}

Mode	Privileged EXEC

debug transfer

M4250

M4350

This command enables debugging for file transfers.

Note: To display the debug trace, enable the debug console command.

Format	debug transfer

Mode	Privileged EXEC

no debug transfer

This command disables debugging for file transfers.

Format	no debug transfer
Mode	Privileged EXEC

debug udd events

M4250

M4350

This command enables debugging for the UDLD events.

To display the debug trace, enable the debug console command.

Default	Disabled
Format	debug udd events
Mode	Privileged EXEC

no debug udd events

This command disables debugging for the UDLD events.

Format	no debug udd events
Mode	Privileged EXEC

debug udd packet

M4250

M4350

This command enables debugging on the received or transmitted UDLD PDUs, or both.

Note: To display the debug trace, enable the debug console command.

Default	Disabled
Format	debug udd packet [receive transmit]
Mode	Privileged EXEC

no debug udld packet

This command disables debugging for UDLD packets.

Format	no debug udld packet [receive transmit]

Mode	Privileged EXEC

debug ipdt logging

M4250

M4350

This command enables debug tracing for IPv4DT events. Debug messages are sent to the system log at the debug severity level. To print these messages on the console, enable console logging at the debug level using the **logging console debug** command.

Default	Enabled

Format	debug ipdt logging

Mode	Privileged Config

no debug ipdt logging

This command disables debug tracing for IPv4DT events.

Format	no debug ipdt logging

Mode	Privileged Config

debug ip vrrp

M4350

This command enables debug tracing of VRRP events. Debug messages are sent to the system log at the debug severity level. To print these messages on the console, enable console logging at the debug level with the **logging console debug** command.

The debug options that are enabled for a specific peer are the sum of the options that are enabled globally and the options that are enabled specifically for the peer.

Default	Disabled

Format	debug ip vrrp

Mode	Privileged Config

no debug ip vrrp

This command disables debug tracing of VRRP events.

Format	no debug ip vrrp
Mode	Privileged Config

debug ipv6 ospfv3 packet

M4350

This command enables IPv6 OSPFv3 packet debug tracing. As an option, use the **vrf** keyword and associated *vrf-name* argument to enable tracing of OSPFv3 packets that are received and transmitted on a specific virtual router instance.

Default	Disabled
Format	debug ipv6 ospfv3 packet [<i>vrf vrf-name</i>]
Mode	Privileged Config

no debug ipv6 ospfv3 packet

This command disables debug tracing of IPv6 OSPFv3 packets.

Format	no debug ipv6 ospfv3 packet
Mode	Privileged Config

debug ipv6 ping packet

M4250

M4350

This command enables debug tracing of ICMPv6 Echo request and response packets. As an option, use the **vrf** keyword and associated *vrf-name* argument to enable tracing of ICMPv6 Echo request and response packets that are received and transmitted on a specific virtual router instance.

Default	Disabled
Format	debug ipv6 ping packet [<i>vrf vrf-name</i>]
Mode	Privileged Config

no debug ipv6 ping packet

This command disables debug tracing of ICMPv6 Echo request and response packets.

Format	no debug ipv6 ping packet

Mode	Privileged Config

show debugging

M4250

M4350

Use this command to display enabled packet tracing configurations.

Format	show debugging

Mode	Privileged EXEC

Command example:

```
console# debug arp
Arp packet tracing enabled.
```

```
console# show debugging
Arp packet tracing enabled.
```

no show debugging

Use this command to disable packet tracing configurations.

Format	no show debugging

Mode	Privileged EXEC

exception protocol

M4250

M4350

Use this command to specify the protocol used to store the core dump file.

Default	usb

Format	exception protocol {nfs tftp ftp usb local}

Mode	Global Config

no exception protocol

Use this command to reset the exception protocol configuration to its factory default value.

Format	no exception protocol
Mode	Global Config

exception dump ftp-server

M4250

M4350

Use this command to configure the IP address of a remote FTP server as an external server to which you can dump core files. If you do not specify the user name and password, the switch uses anonymous FTP. (The FTP server must be configured to accept anonymous FTP.)

Default	None
Format	exception dump ftp-server <i>ip-address</i> [{username <i>user-name</i> password <i>password</i> }]
Mode	Global Config

no exception dump ftp-server

This command resets the remote FTP server configuration that is used for exception dumps to the default value (which is none). This command also resets the FTP user name and password to empty strings.

Format	exception dump ftp-server
Mode	Global Config

exception dump tftp-server

M4250

M4350

Use this command to configure the IP address of a remote TFTP server in order to dump core files to an external server.

Default	None
Format	exception dump tftp-server { <i>ip-address</i> }
Mode	Global Config

no exception dump tftp-server

Use this command to reset the exception dump remote server configuration to its factory default value.

Format	no exception dump tftp-server

Mode	Global Config

exception dump filepath

M4250

M4350

Use this command to configure a file-path to dump core file to a TFTP server, FTP server, NFS mount, or USB device subdirectory.

Default	None

Format	exception dump filepath <i>dir</i>

Mode	Global Config

no exception dump filepath

Use this command to reset the exception dump filepath configuration to its factory default value.

Format	no exception dump filepath

Mode	Global Config

exception dump compression

M4250

M4350

Use this command to enable compression mode.

Default	Enabled

Format	exception dump compression

Mode	Global Config

no exception dump compression

This command disables compression mode.

Format	no exception dump compression
Mode	Global Config

exception dump stack-ip-address protocol

M4250

M4350

This command configures the protocol (DHCP or static) that is used to configure the service port after a unit crashed. If you enter the **dhcp** keyword, the unit receives its IP address from a DHCP server that must be available in the network.

Default	dhcp
Format	exception dump stack-ip-address protocol {dhcp static}
Mode	Global Config

no exception dump stack-ip-address protocol

This command resets the stack IP protocol configuration to its default value (dhcp).

Format	no exception dump stack-ip-address protocol
Mode	Global Config

exception dump stack-ip-address add

M4250

M4350

Use this command to add a static IP address that is assigned to an individual unit's service port in a stack after the unit crashed. This IP address is used to perform the core dump.

Default	None
Format	exception dump stack-ip-address add <i>ip-address netmask [gateway]</i>
Mode	Global Config

exception dump stack-ip-address remove

M4250**M4350**

Use this command to remove a stack IP address configuration. If this IP address is assigned to any unit in a stack then, the IP address is removed from the unit.

Format	<code>no exception dump stack-ip-address remove ip-address netmask</code>
Mode	Global Config

exception core-file

M4250**M4350**

Use this command to configure a prefix for a core-file name. The core file name is generated with the prefix as follows:

If **hostname** is selected:

`file-name-prefix_hostname_Time_Stamp.bin`

If **hostname** is not selected:

`file-name-prefix_MAC_Address_Time_Stamp.bin`

If **hostname** is configured, the core file name takes the host name, otherwise the core-file names uses the MAC address when generating a core dump file. The prefix length is 15 characters.

Default	Core
Format	<code>exception core-file file-name [hostname] [time-stamp]</code>
Mode	Global Config

no exception core-file

Use this command to reset the exception core file prefix configuration to its factory default value. The hostname and time-stamp are disabled.

Format	<code>no exception core-file</code>
Mode	Global Config

exception switch-chip-register

M4250**M4350**

Use this command to enable or disable the switch-chip-register dump in case of an exception. For an M4350 series switch in a switch stack, the switch-chip-register dump occurs only for the primary management unit and not for members.

Default	Disable
Format	exception switch-chip-register {enable disable}
Mode	Global Config

write core

M4250**M4350**

Use this command to generate a core dump file on demand. The **write core test** command is helpful when testing the core dump setup. For example, if the TFTP protocol is configured, **write core test** communicates with the TFTP server and informs the user if the TFTP server can be contacted. Similarly, if the protocol is configured as **nfs**, this command mounts and unmounts the file system and informs the user of the status.

Note: The **write core** command reloads the switch which is useful when the device malfunctions, but has not crashed.

For the **write core test** command, the destination file name is used for the TFTP test. Optionally, you can specify the destination file name when the protocol is configured as TFTP.

Default	None
Format	write core [test <i>file_name</i>]
Mode	Privileged EXEC

debug exception

M4250**M4350**

Use this command to display core dump features support.

Default	None
Format	debug exception
Mode	Privileged EXEC

show exception

M4250**M4350**

Use this command to display the configuration parameters for generating a core dump file.

The optional **core-dump-file** keyword displays core dump files that exist on the local file system. The optional **log** keyword displays core dump traces that exist on the local file system.

Default	None
Format	show exception [core-dump-file log [previous]]
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show exception
```

```

Coredump file name..... core
Coredump filename uses hostname..... False
Coredump filename uses time-stamp..... TRUE
NFS mount point.....
TFTP server IP.....
FTP server IP.....
FTP user name.....
FTP password.....
File path.....
Protocol..... usb
Switch-chip-register..... False
Compression mode..... TRUE
Stack IP Address Protocol..... dhcp
Stack IP Address:
IP Address      Net Mask      Gateway      Assigned Unit
-----

```

mbuf

M4250

M4350

Use this command to configure memory buffer (MBUF) threshold limits and generate notifications when MBUF limits have been reached.

Format	mbuf {falling-threshold 1-100 rising threshold 1-100 severity 0-7}
Mode	Global Config
Parameter	Description
Rising Threshold	The percentage of the memory buffer resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Falling Threshold	The percentage of memory buffer resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Severity	The severity level at which Mbuf logs messages. The range is 1 to 7. The default is 5 (L7_LOG_SEVERITY_NOTICE).

show mbuf

M4250

M4350

Use this command to display the memory buffer (MBUF) Utilization Monitoring parameters.

Format	show mbuf
Mode	Privileged EXEC
Field	Description
Rising Threshold	The percentage of the memory buffer resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Falling Threshold	The percentage of memory buffer resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Severity	The severity level.

show mbuf total

M4250

M4350

Use this command to display memory buffer (MBUF) information.

Format	show mbuf total
Mode	Privileged EXEC
Field	Description
Mbufs Total	Total number of message buffers in the system.
Mbufs Free	Number of message buffers currently available.
Mbufs Rx Used	Number of message buffers currently in use.
Total Rx Norm Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Norm.
Total Rx Mid2 Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Mid2.
Total Rx Mid1 Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Mid1.
Total Rx Mid0 Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Mid0.
Total Rx High Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX High.
Total Tx Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class TX.
Total Rx Norm Alloc Failures	Number of message buffer allocation failures for RX Norm class of message buffer.
Total Rx Mid2 Alloc Failures	Number of message buffer allocation failures for RX Mid2 class of message buffer.
Total Rx Mid1 Alloc Failures	Number of message buffer allocation failures for RX Mid1 class of message buffer.
Total Rx Mid0 Alloc Failures	Number of message buffer allocation failures for RX Mid0 class of message buffer.
Total Rx High Alloc Failures	Number of message buffer allocation failures for RX High class of message buffer.
Total Tx Alloc Failures	Number of message buffer allocation failures for TX class of message buffer.

clear mbuf stats

M4250

M4350

Use this command to delete the memory buffer (MBUF) statistics.

Format	clear mbuf stats
Mode	Privileged Exec

Command example:

```
(NETGEAR Switch)#clear mbuf stats
```

```
Are you sure you want to clear mbuf statistics (y/n) y
```

```
mbuf stats cleared.
```

show msg-queue

M4250

M4350

Use this command to display the message queues.

Default	None
Format	show msg-queue
Mode	Privileged Exec

session start

M4350

Use this command to initiate a console session from the stack primary management unit to another unit in the stack, or from a member unit to a manager or another member unit. During the session, you can issue troubleshooting and debugging commands on the member unit, and the output displays the relevant information from the member unit specified in the session. Commands are displayed on the member unit using the user help option ?.

Use the **unit** keyword and *unit-number* parameter to specify the unit that must connect to the primary management unit.

Use the **manager** keyword to connect directly to the manager unit from any member unit without entering the manager's unit number.

Default	Disabled
Format	<code>session start {unit <i>unit-number</i> manager}</code>
Mode	Privileged Exec

session stop

M4350

Use this command to terminate a session that was started with the **session start** command. The session can be from a manager to a member, from member to a member, or from a member to a manager.

Use the **unit** keyword and *unit-number* argument to specify the unit that must disconnect from the primary management unit.

Use the **manager** keyword to disconnect directly from the manager unit from any member unit without entering the manager's unit number.

Default	Disabled
Format	<code>session stop {unit <i>unit-number</i> manager}</code>
Mode	Global Config

sw reset

M4250

M4350

Use this command to reboot the switch after a serious error occurred.

Default	Enabled
Format	<code>sw reset</code>
Mode	Global Config

no sw reset

Use this command to prevent the switch from rebooting after a serious error occurred. Preventing the switch from rebooting can be useful for the purpose of debugging.

Format	<code>no sw reset</code>
Mode	Global Config

show sw reset

M4250

M4350

Use this command to show whether the **sw reset** command is enabled.

Format	show sw reset
Mode	Privileged Exec

Cable Test Command

The cable test feature enables you to determine the cable connection status on a selected port.

Note: The cable test feature is supported only for copper cables. It is not supported for optical fiber cables.

If the port has an active link while the cable test is run, the link can go down for the duration of the test.

cablestatus

M4250

M4350

This command returns the status of the specified port.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	cablestatus <i>unit/slot/port</i>
Mode	Privileged EXEC

Field	Description
Cable Status	One of the following statuses is returned: • <code>Normal</code>. The cable is working correctly. • <code>Open</code>. The cable is disconnected or there is a faulty connector. • <code>Short</code>. There is an electrical short in the cable. • <code>Cable Test Failed</code>. The cable status could not be determined. The cable may in fact be working.
Cable Length	If this feature is supported by the PHY for the current link speed, the cable length is displayed as a range between the shortest estimated length and the longest estimated length. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter, then the cable status may display as <code>Open</code> or <code>Short</code> because some Ethernet adapters leave unused wire pairs unterminated or grounded. <code>Unknown</code> is displayed if the cable length could not be determined.

Power Management Commands

Note: Power management commands are supported on the M4350 series switches only. The M4250 series switches do not support power management commands.

power redundancy

M4350

This command enables the N+1 power redundancy feature on a switch with a dual PSU configuration. If this feature is enabled, only one PSU provides PoE power to the switch. If the PSU fails, the redundant PSU seamlessly takes over the supply of PoE power to the switch. If this command is disabled, N+1 is also disabled and both PSUs provide PoE power to the switch at the same time. In this situation, the PoE budget for the switch increases.

The *unit-number* argument specifies the PSU in the switch.

Default	Disabled
Format	<code>power redundancy [unit-number]</code>
Mode	Global Config

Note: If the total available power minus the total consumed power is less than what one PSU can supply, the switch does not enable the N+1 feature. Instead, it generates the following error message on the console and in the logging buffer:

```
Not enough power to enable N+1 feature. Total
available power: <X>. Total consumption power: <Y>
```

no power redundancy

This command disables the N+1 power redundancy feature.

Format	no power redundancy

Mode	Global Config

show power redundancy

M4350

This command displays the power redundancy status.

Format	show power redundancy

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch)# show power redundancy
N+1 configuration: ..... Disable
N+1 Active: ..... No
Number of PSU: ..... 1
Effective Number of PSU: ..... 1
```

show power

M4350

This command displays the switch power usage.

The optional *unit-number* argument specifies the PSU in the switch.

Format	show power [<i>unit-number</i>]

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show power

Unit : 1
Model Name:..... M4350-16V4C
Total Available power(W): ..... 420
Total Power Module Slot Number:..... 2
```

Power			Power	
Modules	Module		Module	
Slot	Name	Status	AC Input (V)	
-----	-----	-----	-----	

1		Not Present	
2	APS420W	Operational	100-240

USB commands

If your switch model includes a USB slot and a USB flash device is installed in the USB slot, the USB commands display the device status and content.

show usb device

M4250

M4350

This command displays USB flash device details.

Format	show USB device
Mode	Privileged EXEC
Term	Description
Device Status	This field specifies the current status of device. Following are possible device status states: - Active. Device is plugged in and the device is recognized if device is not mounted. - Inactive. Device is not mounted. - Invalid. Device is not present or invalid device is plugged in.

Command example:

```
(NETGEAR Switch) #show USB device
```

```
Device Status..... Active
```

dir usb

M4250

M4350

This command displays USB device contents and memory statistics.

Format	dir usb
Mode	Privileged EXEC

Term	Description
Filename	File name
Filesize	File size
Total Size	USB flash device storage size
Bytes Used	Indicates size of memory used on the device.
Bytes Free	Indicates size of memory free on the device

Command example:

```
(NETGEAR Switch) #dir USB:
Filename Filesize  Modification Time
Fl.cfg   256        4/22/2009 8:00:12
```

```
Total Size: xxxx
Bytes Used: yyyy
Bytes Free: zzzz
```

unmount usb**M4250****M4350**

This command lets you unmount a USB device. This command works only if your switch model includes at least one USB port in which a USB device is installed. If your switch model includes two USB ports, you can specify the UBS device number (1 or 2).

Format	unmount usb [1 2]
Mode	Privileged EXEC

logging usb**M4250****M4350**

This command configures the logging severity level for a USB device that is installed in the switch. This command works only if your switch model includes at least one USB port in which a USB device is installed.

For the *severitylevel* argument, enter one of the followings:

- emergency: 0
- alert: 1
- critical: 2
- error: 3

- warning: 4
- notice: 5
- info: 6
- debug: 7

Format	<code>logging usb <i>severitylevel</i></code>

Mode	Global Config

logging usb device-number

M4250

M4350

If your switch model includes two USB slots, this command lets you configure USB device logging for one of two USB devices.

This command works only if your switch model includes at least one USB port in which a USB device is installed. If your switch model includes two USB ports, you can specify the USB device number (1 or 2).

Format	<code>logging usb device-number {1 2}</code>

Mode	Privileged EXEC

logging usb overwrite-on-full

M4250

M4350

This command configures USB device logging to overwrite the log when it is full. As an option, you can set the logging severity level. For the *severitylevel* argument, enter one of the followings:

- emergency: 0
- alert: 1
- critical: 2
- error: 3
- warning: 4
- notice: 5
- info: 6
- debug: 7

Format	<code>logging usb overwrite-on-full [<i>severitylevel</i>]</code>

Mode	Privileged EXEC

logging usb stop-on-full

M4250

M4350

This command configures USB device logging to stop writing when the log is full. As an option, you can set the logging severity level. For the *severitylevel* argument, enter one of the followings:

- emergency: 0
- alert: 1
- critical: 2
- error: 3
- warning: 4
- notice: 5
- info: 6
- debug: 7

Format	logging usb stop-on-full [<i>severitylevel</i>]
Mode	Privileged EXEC

sFlow Commands

sFlow is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

sflow receiver

M4250

M4350

Use this command to configure the sFlow collector parameters (owner string, receiver time-out, max datagram size, IP address, and port).

Format	sflow receiver <i>index</i> [<i>maxdatagram size</i> ip <i>ip-address</i> port <i>port-number</i>]
Mode	Global Config

Parameter	Description
Receiver Max Datagram Size	The maximum number of data bytes that can be sent in a single sample datagram. The management entity must set this value to avoid fragmentation of the sFlow datagrams. The allowed range is 200 to 12188 for the M4250 series switch or 12184 for the M4350 series switch. The default is 1400.
Receiver IP	The sFlow receiver IP address. If set to 0.0.0.0, no sFlow datagrams is sent. The default is 0.0.0.0.
Receiver Port	The destination Layer4 UDP port for sFlow datagrams. The range is 1-65535. The default is 6343.

no sflow receiver

Use this command to set the sFlow collector parameters back to the defaults.

Format	no sflow receiver <i>index</i> [maxdatagram ip port]
Mode	Global Config

sflow receiver owner

M4250

M4350

Use this command to configure an sFlow receiver as a timeout or non-timeout entry:

- **timeout:** Use this keyword to configure an sFlow receiver as a timeout entry. Information related to samplers and pollers are also shown in the `running-config` file and are retained after a reboot.
- **non-timeout:** Use this command to configure an sFlow receiver as a non-timeout entry. Unlike entries configured with a specific timeout value, this command is shown in the output of the `show running-config` command and retained after a reboot. Information related to samplers and pollers is also shown in the `running-config` file and retained after a reboot.

If a receiver is configured with a specific value, these configurations are not shown in the `running-config` file. Samplers and pollers information related to this receiver are also not shown in the `running-config` file.

Format	sflow receiver <i>index</i> owner <i>owner-string</i> {timeout notimeout}
Mode	Global Config

Field	Description
index	Receiver index identifier. The range is 1 to 8.
Receiver Owner	The owner name corresponds to the receiver name. The identity string for the receiver, the entity making use of this sFlowRcvrTable entry. The range is 127 characters. The default is a null string. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the 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 to a non-null value. The entry must be claimed before assigning a receiver to a sampler or poller.

no sflow receiver owner

Use this command to disable an sFlow receiver as a timeout or non-timeout entry.

Format no sflow receiver index owner

Mode Global Config

sflow sampler

M4250

M4350

A data source configured to collect flow samples is called a poller. Use this command to configure a new sFlow sampler instance on an interface or range of interfaces for this data source if the receiver *index* is valid.

Format sflow sampler {index | rate *sampling-rate* | maxheadersize *size*}

Mode Interface Config

Field	Description
Receiver Index	The sFlow Receiver for this sFlow sampler to which flow samples are to be sent. A value of zero (0) means that no receiver is configured, no packets will be sampled. Only active receivers can be set. If a receiver expires, then all samplers associated with the receiver will also expire. Possible values are 1-8. The default is 0.
Maxheadersize	The maximum number of bytes that should be copied from the sampler packet. The range is 20-256. The default is 128. When set to zero (0), all the sampler parameters are set to their corresponding default value.

Field	Description
Sampling Rate	The statistical sampling rate for packet sampling from this source. A value of zero (0) disables sampling. A value of N means that out of N incoming packets, 1 packet will be sampled. The range is 1024-65536 and 0. The default is 0. When you issue a show command for the sampling rate, the configured sampling rate on an interface changes. Each time that you configure a sampling rate, a threshold value is calculated. This threshold value is configured in the hardware register. When you issue a show command for the sampling rate, the threshold value is queried from the hardware and the sampling rate is calculated in the following way: $\text{threshold value} = 2^{24} / (\text{sampling rate})$ Because only an integer operation is supported, the sampling rate is not the same as the configured value. The following is an example: <pre>configured sampling rate is 60000 threshold value = 2^24 / (60000) = 279 (from integer division) recalculated sampling rate = 2^24 / (279) = 60133</pre>

no sflow sampler

Use this command to reset the sFlow sampler instance to the default settings.

Format	<code>no sflow sampler {index rate sampling-rate maxheadersize size}</code>
Mode	Interface Config

sflow poller

M4250

M4350

A data source configured to collect counter samples is called a poller. Use this command to enable a new sFlow poller instance on an interface or range of interfaces for this data source if the receiver *index* is valid.

Format	<code>sflow poller {index interval poll-interval}</code>
Mode	Interface Config

Field	Description
Receiver Index	Enter the sFlow Receiver associated with the sampler/poller. A value of zero (0) means that no receiver is configured. The range is 1-8. The default is 0.
Poll Interval	Enter the sFlow instance polling interval. A poll interval of zero (0) disables counter sampling. When set to zero (0), all the poller parameters are set to their corresponding default value. The range is 0-86400. The default is 0. A value of N means once in N seconds a counter sample is generated.

The sFlow task is heavily loaded when the sFlow polling interval is configured at the minimum value (i.e., one second for all the sFlow supported interfaces). In this case, the sFlow task is always busy collecting the counters on all the configured interfaces. This can

cause the device to hang for some time when the user tries to configure or issue show sFlow commands.

To overcome this situation, sFlow polling interval configuration on an interface or range of interfaces is controlled as mentioned below:

1. The maximum number of allowed interfaces for the polling intervals max (1, (interval – 10)) to min ((interval + 10), 86400) is:
interval * 5
2. For every one second increment in the polling interval that is configured, the number of allowed interfaces that can be configured increases by 5.

no sflow poller

Use this command to reset the sFlow poller instance to the default settings.

Format	no sflow poller [interval]
Mode	Interface Config

sflow source-interface

M4250

M4350

Use this command to specify the physical or logical interface to use as the sFlow client source interface. If configured, the address of source Interface is used for all sFlow communications between the sFlow receiver and the sFlow client. Otherwise there is no change in behavior. If the configured interface is down, the sFlow client falls back to normal behavior.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	sflow source-interface {unit/slot/port loopback loopback-id serviceport vlan vlan-id}
Mode	Global Config

Parameter	Description
slot/port or unit/slot/port	The port-based routing interface is used as the source.
loopback-id	The loopback interface that is used as the source IP address. The range of the loopback ID is 0 to 7.

Parameter	Description
serviceport	The IP address of the service port is used as the source IP address.
vlan-id	The VLAN interface that is used as the source IP address. The range of the VLAN ID is 1 to 4093.

no sflow source-interface

Use this command to reset the sFlow source interface to the default settings.

Format	no sflow source-interface
Mode	Global Config

show sflow agent

M4250

M4350

The sFlow agent collects time-based sampling of network interface statistics and flow-based samples. These are sent to the configured sFlow receivers. Use this command to display the sFlow agent information.

Format	show sflow agent
Mode	Privileged EXEC

Field	Description
sFlow Version	Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: MIB Version; Organization; Software Revision where: MIB Version: 1.3, the version of this MIB. Organization: NETGEAR Corp. Revision: 1.0
IP Address	The IP address associated with this agent.

Command example:

```
(NETGEAR Switch) #show sflow agent
```

```
sFlow Version..... 1.3;NETGEAR Corp;1.0
IP Address..... 10.131.12.66
```

show sflow pollers

M4250

M4350

Use this command to display the sFlow polling instances created on the switch. Use “-” for range.

Format	show sflow pollers
Mode	Privileged EXEC
Field	Description
Poller Data Source	The sFlowDataSource (unit/port) for this sFlow sampler. This agent will support physical ports only.
Receiver Index	The sFlowReceiver associated with this sFlow counter poller.
Poller Interval	The number of seconds between successive samples of the counters associated with this data source.

show sflow receivers

M4250

M4350

Use this command to display configuration information related to the sFlow receivers.

Format	show sflow receivers [index]
Mode	Privileged EXEC
Parameter	Description
Receiver Index	The sFlow Receiver associated with the sampler/poller.
Owner String	The identity string for receiver, the entity making use of this sFlowRcvrTable entry.
Time Out	The time (in seconds) remaining before the receiver is released and stops sending samples to sFlow receiver. The no timeout value of this parameter means that the sFlow receiver is configured as a non-timeout entry.
Max Datagram Size	The maximum number of bytes that can be sent in a single sFlow datagram.
Port	The destination Layer4 UDP port for sFlow datagrams.
IP Address	The sFlow receiver IP address.
Address Type	The sFlow receiver IP address type. For an IPv4 address, the value is 1 and for an IPv6 address, the value is 2.
Datagram Version	The sFlow protocol version to be used while sending samples to sFlow receiver.

Command example:

```
(NETGEAR Switch) #show sflow receivers 1
Receiver Index..... 1
Owner String..... tulasi
Time out..... 0
IP Address:..... 0.0.0.0
Address Type..... 1
Port..... 6343
Datagram Version..... 5
Maximum Datagram Size..... 1400
```

Command example:

The following example shows that a receiver is configured as a non-time-out entry:

```
(NETGEAR Switch) #show sflow receivers
```

Rcvr Indx	Owner String	Timeout	Max Dgram Size	Port	IP Address
1	tulasi	No Timeout	1400	6343	0.0.0.0 <= No Timeout string
2		0	1400	6343	0.0.0.0
3		0	1400	6343	0.0.0.0
4		0	1400	6343	0.0.0.0
5		0	1400	6343	0.0.0.0
6		0	1400	6343	0.0.0.0
7		0	1400	6343	0.0.0.0
8		0	1400	6343	0.0.0.0

Command example:

The following example also shows that a receiver is configured as a non-time-out entry:

```
(NETGEAR Switch) #show sflow receivers 1
```

```
Receiver Index..... 1
Owner String..... tulasi
Time out..... No Timeout      <= No Timeout string
is added
IP Address:..... 0.0.0.0
Address Type..... 1
Port..... 6343
Datagram Version..... 5
Maximum Datagram Size..... 1400
```

show sflow samplers

M4250

M4350

Use this command to display the sFlow sampling instances created on the switch.

Format	show sflow samplers
Mode	Privileged EXEC
Field	Description
Sampler Data Source	The sFlowDataSource (unit/port) for this sFlow sampler. This agent will support physical ports only.
Receiver Index	The sFlowReceiver configured for this sFlow sampler.
Packet Sampling Rate	The statistical sampling rate for packet sampling from this source.
Max Header Size	The maximum number of bytes that should be copied from a sampled packet to form a flow sample.

show sflow source-interface

M4250

M4350

Use this command to display the sFlow source interface configured on the switch.

Format	show sflow source-interface
Mode	Privileged EXEC
Field	Description
sFlow Client Source Interface	The interface ID of the physical or logical interface configured as the sFlow client source interface.
sFlow Client Source IPv4 Address	The IP address of the interface configured as the sFlow client source interface.

Command example:

```
(NETGEAR Switch) #show sflow source-interface
```

```
sFlow Client Source Interface..... (not configured)
```

Switch Database Management Template Commands

Note: Switch Database Management (SDM) template commands are supported on the M4350 series switches only. The M4250 series switches do not support SDM template commands.

A Switch Database Management 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 insert a unit in a stack and its template does not match the template of the stack, the unit reboots automatically using the template that is used by other stack members. To avoid the automatic reboot, first set the template to the template that is used by existing members of the stack. Then power off the new unit, insert it in the stack, and power on the unit.

sdm prefer

M4350

Use this command to change the template that must be active after the next reboot. The keywords are as follows:

- **ipv4-basic.** Template for an IPv4 environment with support for basic IPv6. This is the default template.
- **ipv6-basic.** Template for an IPv6 environment with support for basic IPv4.
- **ipv4-basic-plus.** Template for an IPv4 environment with emphasis on IPv4 unicast and multicast routing and support for IPv6. This template can be used for any M4350 switch model except model M4350-24G4XF.
- **ipv6-basic-plus.** Template for an IPv6 environment with emphasis on IPv6 unicast and multicast routing and support for IPv4. This template can be used for any M4350 switch model except model M4350-24G4XF.
- **ipv4-advanced.** Template for an IPv4 environment which uses mostly IPv4 addresses. Applicable to models M4350-16V4C, M4350-24X8F8V, M4350-36X4V, M4350-32F8V and M4350-40X4C.

- **ipv6-advanced.** Template for an IPv6 environment which uses mostly IPv6 addresses. Applicable to models M4350-16V4C, M4350-24X8F8V, M4350-36X4V, M4350-32F8V and M4350-40X4C.

Note: After setting the template, you must reboot the switch in order for the configuration change to take effect.

Default	IPv4-Basic
Format	sdm prefer {ipv4-basic ipv4-basic-plus ipv4-advanced ipv6-basic ipv6-basic-plus ipv6-advanced}
Mode	Global Config

no sdm prefer

Use this command to revert to the default template after the next reboot.

Format	no sdm prefer
Mode	Global Config

show sdm prefer

M4350

Use this command to view the currently active SDM template and its scaling parameters, or to view the scaling parameters for an inactive template. When invoked with no optional keywords, this command lists the currently active template and the template that will become active on the next reboot, if it is different from the currently active template. If the system boots with a non-default template, and you clear the template configuration, either using **no sdm prefer** or by deleting the startup configuration, **show sdm prefer** lists the default template as the next active template. To list the scaling parameters of a specific template, use that template's keyword as an argument to the command.

The keywords are as follows:

- **ipv4-basic.** Template for an IPv4 environment with support for basic IPv6. This is the default template.
- **ipv6-basic.** Template for an IPv6 environment with support for basic IPv4.
- **ipv4-basic-plus.** Template for an IPv4 environment with emphasis on IPv4 unicast and multicast routing and support for IPv6. This template can be used for any M4350 switch model except model M4350-24G4XF.
- **ipv6-basic-plus.** Template for an IPv6 environment with emphasis on IPv6 unicast and multicast routing and support for IPv4. This template can be used for any M4350 switch model except model M4350-24G4XF.

- **ipv4-advanced.** Template for an IPv4 environment which uses mostly IPv4 addresses. Applicable to models M4350-16V4C, M4350-24X8F8V, M4350-36X4V, M4350-32F8V and M4350-40X4C.
- **ipv6-advanced.** Template for an IPv6 environment which uses mostly IPv6 addresses. Applicable to models M4350-16V4C, M4350-24X8F8V, M4350-36X4V, M4350-32F8V and M4350-40X4C.

Format `show sdm prefer [ipv4-basic | ipv4-basic-plus | ipv4-advanced | ipv6-basic | ipv6-basic-plus | ipv6-advanced]`

Mode Privileged EXEC

Field	Description
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.

Command example:

The following example shows the SDM template when the next active SDM template is not changed:

```
(NETGEAR Switch)#show sdm prefer
```

The current configured template is 'IPv4-Basic'.

Template Summary:

Template Name	ARP Entries	IPv4 Unicast Routes	IPv6 NDP Entries	IPv6 Unicast Routes	ECMP Next Hops	IPv4 Multicast Routes	IPv6 Multicast Routes	Maximum VLAN Entries
IPv4-Basic	4096	894	512	126	16	512	128	4093
IPv6-Basic	512	126	4096	894	16	128	512	4093
IPv4-Advanced	12288	10240	2048	2048	16	2048	512	4093
IPv6-Advanced	2048	2048	12288	10240	16	512	2047	4093

The current template is the 'dual ipv4 and ipv6 data center generic' template.

```
ARP Entries..... 1536
IPv4 Unicast Routes..... 512
IPv6 NDP Entries..... 512
IPv6 Unicast Routes..... 256
ECMP Next Hops..... 4
IPv4 Multicast Routes..... 96
IPv6 Multicast Routes..... 32
```

Maximum VLAN Entries..... 4093

Command example:

The following example shows the SDM template when the next active SDM template is configured:

```
(NETGEAR Switch) sdm prefer ipv6-advanced
```

The current configured template is 'IPv4-Basic'.

Template Summary:

Template Name	ARP Entries	IPv4 Unicast Routes	IPv6 NDP Entries	IPv6 Unicast Routes	ECMP Next Hops	IPv4 Multicast Routes	IPv6 Multicast Routes	Maximum VLAN Entries
IPv4-Basic	4096	894	512	126	16	512	128	4093
IPv6-Basic	512	126	4096	894	16	128	512	4093
IPv4-Advanced	12288	10240	2048	2048	16	2048	512	4093
IPv6-Advanced	2048	2048	12288	10240	16	512	2047	4093

On the next reload, the template will be the 'ipv6-advanced' template.

Green Ethernet Commands

This section describes the commands you use to configure Green Ethernet modes on the system. The purpose of the Green Ethernet features is to save power. The switch supports the following Green Ethernet modes:

- Energy-detect mode
- Energy-efficient Ethernet (EEE) mode

Note: Energy-detect mode is supported on 1G copper ports only.

green-mode energy-detect

M4250

M4350

Use this command to enable energy-detect mode on an interface or on a range of interfaces. With this mode enabled, when the port link is down, the port automatically powers down for short period of time and then wakes up to check link pulses. In energy-detect mode, the port can perform auto-negotiation and consume less power when no link partner is present.

Default	disabled

Format	<code>green-mode energy-detect</code>

Mode	Interface Config

`no green-mode energy-detect`

Use this command to disable energy-detect mode on the interface(s).

Format	<code>no green-mode energy-detect</code>

Mode	Interface Config

`green-mode eee`

M4250

M4350

Use this command to enable EEE low-power idle mode on an interface or on a range of interfaces. The EEE mode enables both send and receive sides of the link to disable some functionality for power saving when lightly loaded. The transition to EEE low-power mode does not change the port link status. Frames in transit are not dropped or corrupted in transition to and from this mode.

Default	disabled

Format	<code>green-mode eee</code>

Mode	Interface Config

`no green-mode eee`

Use this command to disable EEE mode on the interface(s).

Format	<code>no green-mode eee</code>

Mode	Interface Config

`green-mode eee tx-idle-time`

M4250

M4350

Use this command to configure the EEE mode transmit idle time for an interface or range of interfaces. The idle time is in microseconds (0–4294977295). The transmit idle time is the amount of time the port waits before moving to the MAC TX transitions to the LPI state.

Default	0

Format	<code>green-mode eee tx-idle-time <i>microseconds</i></code>

Mode	Interface Config

no green-mode eee tx-idle-time

Use this command to return the EEE idle time to the default value.

Format	no green-mode eee tx-idle-time
Mode	Interface Config

green-mode eee tx-wake-time

M4250

M4350

Use this command to configure the EEE mode transmit wake time for an interface or range of interfaces. The wake time is in microseconds (0–65535). The transmit wake time is the amount of time the switch must wait to go back to the ACTIVE state from the LPI state when it receives a packet for transmission.

Default	0
Format	green-mode eee tx-wake-time <i>microseconds</i>
Mode	Interface Config

no green-mode eee tx-wake-time

Use this command to return the EEE wake time to the default value.

Format	no green-mode eee tx-wake-time
Mode	Interface Config

green-mode eee-lpi-history sampling-interval

M4250

M4350

Use this command to configure global EEE LPI history collection interval for the system. The value specified in this command is applied globally on all interfaces in the switch. The sampling interval unit is seconds (30–36000).

The sampling interval takes effect immediately; the current and future samples are collected at this new sampling interval.

Default	3600 seconds
Format	green-mode eee-lpi-history <i>seconds</i>
Mode	Global Config

no green-mode eee-lpi-history sampling-interval

Use this command to return the global EEE LPI history collection interval to the default value.

Format	no green-mode eee-lpi-history sampling-interval

Mode	Global Config

green-mode eee-lpi-history max-samples

M4250

M4350

Use this command to configure global EEE LPI history collection buffer size for the system. The *size* value (1–168) specified in this command is applied globally on all interfaces in the switch.

Default	168

Format	green-mode eee-lpi-history max-samples <i>size</i>

Mode	Global Config

no green-mode eee-lpi-history max samples

Use this command to return the global EEE LPI history collection buffer size to the default value.

Format	no green-mode eee-lpi-history max-samples

Mode	Global Config

show green-mode

M4250

M4350

Use this command to display the green-mode configuration and operational status on all ports or on the specified port.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Note: The fields that display in the **show green-mode** command output depend on the Green Ethernet modes available on the hardware platform.

Format `show green-mode [unit/slot/port]`

Mode Privileged EXEC

If you do not specify a port, the command displays the information in the following table.

Term	Definition
Global	
Cumulative Energy Saving per Stack	Estimated cumulative energy saved in the stack in (watts * hours) due to all green modes enabled.
Current Power Consumption per Stack	Power consumption by all ports in the stack in mWatts.
Power Saving	Estimated percentage power saved on all ports in the stack due to Green mode(s) enabled.
Unit	Unit Index of the stack member.
Green Ethernet Features supported	List of Green Features supported on the unit which could be one or more of the following: Energy-Detect (Energy Detect), EEE (Energy Efficient Ethernet), LPI-History (EEE Low Power Idle History), LLDP-Cap-Exchg (EEE LLDP Capability Exchange), Pwr-Usg-Est (Power Usage Estimates).
Energy Detect	
Energy-detect Config	Energy-detect Admin mode is enabled or disabled
Energy-detect Opr	Energy detect mode is currently active or inactive. The energy detect mode may be administratively enabled, but the operational status may be inactive.
EEE	
EEE Config	EEE Admin Mode is enabled or disabled.

Command example:

The following example shows that the system supports all green Ethernet features:

```
(NETGEAR Switch) (Config)#show green-mode

Current Power Consumption /Stack (mW)..... 12259

Percentage Power Saving /Stack (%)..... 0

Cumulative Energy Saving /Stack (W * H)..... 0
```

Fully Managed Switches M4250 and M4350 Series

Unit Green Ethernet Features Supported

1 Energy-Detect EEE LPI-History LLDP-Cap-Exchg Pwr-Usg-Est

Interface	Energy-Detect		EEE
	Config	Opr	Config
1/0/1	Disabled	Inactive	Disabled
1/0/2	Disabled	Inactive	Disabled
1/0/3	Disabled	Inactive	Disabled
1/0/4	Disabled	Inactive	Disabled
1/0/5	Disabled	Inactive	Disabled
1/0/6	Disabled	Inactive	Disabled
1/0/7	Disabled	Inactive	Disabled
1/0/8	Disabled	Inactive	Disabled
1/0/9	Disabled	Inactive	Disabled

If you specify the port, the command displays the information in the following table.

Term	Definition
Energy Detect	
Energy-detect admin mode	Energy-detect mode is enabled or disabled
Energy-detect operational status	Energy detect mode is currently active or inactive. The energy-detect mode may be administratively enabled, but the operational status may be inactive. The possible reasons for the status are described below.
Reason for Energy-detect current operational status	The energy detect mode may be administratively enabled, but the operational status may be inactive for one of the following reasons: - Port is currently operating in the fiber mode - Link is up. - Admin Mode Disabled If the energy-detect operational status is active, this field displays <i>No energy detected</i>.
EEE	
EEE Admin Mode	EEE Admin Mode is enabled or disabled.
Transmit Idle Time	It is the time for which condition to move to LPI state is satisfied, at the end of which MAC TX transitions to LPI state. The Range is (0 to 429496729). The Default value is 0
Transmit Wake Time	It is the time for which MAC / switch has to wait to go back to ACTIVE state from LPI state when it receives packet for transmission. The Range is (0 to 65535).The Default value is 0.
Rx Low Power Idle Event Count	This field is incremented each time MAC RX enters LP IDLE state. Shows the total number of Rx LPI Events since EEE counters are last cleared.

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Rx Low Power Idle Duration (μSec)	This field indicates duration of Rx LPI state in 10 μs increments. Shows the total duration of Rx LPI since the EEE counters are last cleared.
Tx Low Power Idle Event Count	This field is incremented each time MAC TX enters LP IDLE state. Shows the total number of Tx LPI Events since EEE counters are last cleared.
Rx Low Power Idle Duration (μSec)	This field indicates duration of Tx LPI state in 10 μs increments. Shows the total duration of Tx LPI since the EEE counters are last cleared.
Tw_sys_tx (μSec)	Integer that indicates the value of Tw_sys that the local system can support. This value is updated by the EEE DLL Transmitter state diagram.
Tw_sys Echo (μSec)	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 (μSec)	Integer that indicates the value of Tw_sys that the local system requests from the remote system. This value is updated by the EEE Receiver L2 state diagram.
Tw_sys_rx Echo (μSec)	Integer that indicates the remote systems Receive Tw_sys that was used by the local system to compute the Tw_sys that it can support.
Fallback Tw_sys (μSec)	Integer that indicates the value of fallback Tw_sys that the local system requests from the remote system.
Remote Tw_sys_tx (μSec)	Integer that indicates the value of Tw_sys that the remote system can support.
Remote Tw_sys Echo (μSec)	Integer that indicates the value Transmit Tw_sys echoed back by the remote system.
Remote Tw_sys_rx (μSec)	Integer that indicates the value of Tw_sys that the remote system requests from the local system.
Remote Tw_sys_rx Echo (μSec)	Integer that indicates the value of Receive Tw_sys echoed back by the remote system.
Remote Fallback Tw_sys (μSec)	Integer that indicates the value of fallback Tw_sys that the remote system is advertising.
Tx_dll_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. This variable is updated by the local system software.
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. This variable is updated by the local system software.
Cumulative Energy Saving	Estimated Cumulative energy saved on this port in (Watts × hours) due to all green modes enabled
Time Since Counters Last Cleared	Time Since Counters Last Cleared (since the time of power up, or after the clear eee statistics command is executed)

Command example:

The following example shows that the system supports all green Ethernet features:

```
(NETGEAR Switch) #show green-mode 1/0/1
Energy Detect Admin Mode..... Enabled
Operational Status..... Active
Reason..... No Energy Detected

Auto Short Reach Admin Mode..... Enabled
Forced Short Reach Admin Mode..... Enabled
Operational Status..... Active
Reason..... Forced

EEE Admin Mode..... Enabled
Transmit Idle Time..... 0
Transmit Wake Time..... 0
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)..... XX
Tw_sys_tx Echo(uSec)..... XX
Tw_sys_rx (uSec)..... XX
Tw_sys_tx Echo(uSec)..... XX
Fallback Tw_sys (uSec)..... XX
Remote Tw_sys_tx (uSec)..... XX
Remote Tw_sys_tx Echo(uSec)..... XX
Remote Tw_sys_rx (uSec)..... XX
Remote Tw_sys_tx Echo(uSec)..... XX
Remote fallback Tw_sys (uSec)..... XX
Tx DLL enabled..... Yes
Tx DLL ready..... Yes
Rx DLL enabled..... Yes
Rx DLL ready..... Yes
Cumulative Energy Saving (W * H)..... XX
Time Since Counters Last Cleared..... 1 day 20 hr 47 min 34 sec
```

show green-mode eee-lpi-history

M4250

M4350

Use this command to display interface green-mode EEE LPI history.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.

- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>green-mode eee-lpi-history interface <i>unit/slot/port</i></code>
Mode	Privileged EXEC
Term	Definition
Sampling Interval	Interval at which EEE LPI statistics is collected.
Total No. of Samples to Keep	Maximum number of samples to keep.
Percentage LPI time per switch	Percentage of total time spent in LPI mode by all port in a switch when compared to total time since reset.
Sample No.	Sample Index.
Sample Time	Time since last reset.
%time spent in LPI mode since last sample	Percentage of time spent in LPI mode on this port when compared to sampling interval.
%time spent in LPI mode since last reset	Percentage of total time spent in LPI mode on this port when compared to time since reset.

Command example:

The following example shows that the system has the EEE feature enabled:

```
(NETGEAR Switch) #show green-mode eee-lpi-history interface 1/0/1
```

```
Sampling Interval (sec)..... 30
Total No. of Samples to Keep..... 168
Percentage LPI time per Stack..... 29
```

Sample No.	Time Since The Sample Was Recorded	Percentage of Time spent in LPI mode since last sample	Percentage of Time spent in LPI mode since last reset
10	0d:00:00:13	3	2
9	0d:00:00:44	3	2
8	0d:00:01:15	3	2
7	0d:00:01:46	3	2
6	0d:00:02:18	3	2
5	0d:00:02:49	3	2
4	0d:00:03:20	3	2
3	0d:00:03:51	3	1
2	0d:00:04:22	3	1
1	0d:00:04:53	3	1

clear green-mode statistics

M4250

M4350

Use this command to clear the following Green Ethernet mode statistics:

- EEE LPI event count and LPI duration
- EEE LPI history table entries
- Cumulative power-savings estimates

You can clear the statistics for a specified port or for all ports.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Note: Executing `clear eee statistics` clears only the EEE Transmit, Receive LPI event count, LPI duration, and Cumulative Energy Savings Estimates of the port. Other status parameters that display after executing `show green-mode` (see [show green-mode on page 447](#)) retain their data.

Format	<code>clear green-mode statistics {unit/slot/port all}</code>
Mode	Privileged EXEC

Remote Monitoring Commands

Remote Monitoring (RMON) is a method of collecting a variety of data about network traffic. RMON supports 64-bit counters (RFC 3273) and High Capacity Alarm Table (RFC 3434).

Note: There is no configuration command for ether stats and high capacity ether stats. The data source for ether stats and high capacity ether stats are configured during initialization.`rmon alarm`

rmon alarm

M4250

M4350

This command sets the RMON alarm entry in the RMON alarm MIB group.

Format `rmon alarm alarm-number variable sample-interval {absolute | delta} rising-threshold value [rising-event-index] falling-threshold value [falling-event-index] [startup {rising | falling | rising-falling}] [owner string]`

Mode	Global Config

Parameter	Description
Alarm Index	An index that uniquely identifies an entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device. The range is 1 to 65535.
Alarm Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
Alarm Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.
Alarm Absolute Value	The value of the statistic during the last sampling period. This object is a read-only, 32-bit signed value.
Alarm Rising Threshold	The rising threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
Alarm Rising Event Index	The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
Alarm Falling Threshold	The falling threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
Alarm Falling Event Index	The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.
Alarm Startup Alarm	The alarm that may be sent. Possible values are rising, falling or both rising-falling. The default is rising-falling.
Alarm Owner	The owner string associated with the alarm entry. The default is monitorAlarm.

Command example:

```
(NETGEAR Switch) (Config)# rmon alarm 1 ifInErrors.2 30 absolute rising-threshold 100 1
falling-threshold 10 2 startup rising owner myOwner
```

no rmon alarm

This command deletes the RMON alarm entry.

Format no rmon alarm *alarm-number*

Mode Global Config

Command example:

```
(NETGEAR Switch) (Config)# no rmon alarm 1
```

rmon hcalarm

M4250

M4350

This command sets the RMON hcalarm entry in the High Capacity RMON alarm MIB group.

Format rmon hcalarm *alarm-number variable sample-interval* {absolute | delta}
 rising-threshold high value low value status {positive | negative}
 [*rising-event-index*] falling-threshold high value low value status {positive
 | negative} [*falling-event-index*] [startup {rising | falling |
 rising-falling}] [owner *string*]

Mode Global Config

Parameter	Description
High Capacity Alarm Index (<i>alarm-number</i>)	An arbitrary integer index value used to uniquely identify the high capacity alarm entry. The range is 1 to 65535.
High Capacity Alarm Variable (<i>variable</i>)	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
High Capacity Alarm Interval (<i>sample-interval</i>)	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.
High Capacity Alarm Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds. Possible types are absolute and delta . The default is absolute .
High Capacity Alarm Absolute Value	The absolute value (that is, the unsigned value) of the hcAlarmVariable statistic during the last sampling period. The value during the current sampling period is not made available until the period is complete. This object is a 64-bit unsigned value that is Read-Only.
High Capacity Alarm Absolute Alarm Status	This object indicates the validity and sign of the data for the high capacity alarm absolute value object (hcAlarmAbsValueobject). Possible status types are valueNotAvailable, valuePositive, or valueNegative. The default is valueNotAvailable.
High Capacity Alarm Startup Alarm	High capacity alarm startup alarm that may be sent. Possible values are rising , falling , or rising-falling . The default is rising-falling .

Fully Managed Switches M4250 and M4350 Series

Parameter	Description
High Capacity Alarm Rising-Threshold Absolute Value Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
High Capacity Alarm Rising-Threshold Absolute Value High	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
High Capacity Alarm Rising-Threshold Value Status	This object indicates the sign of the data for the rising threshold, as defined by the objects hcAlarmRisingThresAbsValueLow and hcAlarmRisingThresAbsValueHigh. Possible values are valueNotAvailable, valuePositive, or valueNegative. The default is valuePositive.
High Capacity Alarm Falling-Threshold Absolute Value Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
High Capacity Alarm Falling-Threshold Absolute Value High	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
High Capacity Alarm Falling-Threshold Value Status	This object indicates the sign of the data for the falling threshold, as defined by the objects hcAlarmFallingThresAbsValueLow and hcAlarmFallingThresAbsValueHigh. Possible values are valueNotAvailable, valuePositive, or valueNegative. The default is valuePositive.
High Capacity Alarm Rising Event Index	The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
High Capacity Alarm Falling Event Index	The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.
High Capacity Alarm Failed Attempts	The number of times the associated hcAlarmVariable instance was polled on behalf of the hcAlarmEntry (while in the active state) and the value was not available. This object is a 32-bit counter value that is read-only.
High Capacity Alarm Owner	The owner string associated with the alarm entry. The default is monitorHCArm.
High Capacity Alarm Storage Type	The type of non-volatile storage configured for this entry. This object is read-only. The default is volatile.

Command example:

```
(NETGEAR Switch) (Config)# rmon hcalarm 1 ifInOctets.1 30 absolute rising-threshold high
1 low 100 status positive 1 falling-threshold high 1 low 10 status positive startup
rising owner myOwner
```

no rmon hcalarm

This command deletes the rmon hcalarm entry.

Format	no rmon hcalarm <i>alarm-number</i>

Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config)# no rmon hcalarm 1
```

rmon event

M4250

M4350

This command sets the RMON event entry in the RMON event MIB group.

Format	<code>rmon event event-number [description string log owner string trap community]</code>

Mode	Global Config

Parameter	Description
Event number	An index that uniquely identifies an entry in the event table. Each such entry defines one event that is to be generated when the appropriate conditions occur. The range is 1 to 65535.
Description	A comment describing the event entry. The default is alarmEvent.
Log	Creates a log entry.
Owner	The owner string that is associated with the entry. The default is monitorEvent.
Community	The SNMP community, which is specified by an octet string that is used to send an SNMP trap. The default is public.

Command example:

```
(NETGEAR Switch) (Config)# rmon event 1 log description test
```

no rmon event

This command deletes the rmon event entry.

Format	<code>no rmon event event-number</code>

Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config)# no rmon event 1
```

rmon collection history

M4250**M4350**

This command sets the history control parameters of the RMON historyControl MIB group.

Note: This command is not supported on an interface range. Each RMON history control collection entry can be configured on only one interface. If you try to configure on multiple interfaces, the switch displays an error message.

Format	rmon collection history <i>index-number</i> [<i>buckets number</i> <i>interval seconds</i> <i>owner string</i>]

Mode	Interface Config

Parameter	Description
History Control Index	An index that uniquely identifies an entry in the historyControl table. Each such entry defines a set of samples at a particular interval for an interface on the device. The range is 1 to 65535.
History Control Data Source	The source interface for which historical data is collected.
History Control Buckets Requested	The requested number of discrete time intervals over which data is to be saved. The range is 1 to 65535. The default is 50.
History Control Buckets Granted	The number of discrete sampling intervals over which data shall be saved. This object is read-only. The default is 10.
History Control Interval	The interval in seconds over which the data is sampled. The range is 1 to 3600. The default is 1800.
History Control Owner	The owner string associated with the history control entry. The default is monitorHistoryControl.

Command example:

```
(NETGEAR Switch) (Interface 1/0/1)# rmon collection history 1 buckets 10 interval 30
owner myOwner
```

Command example:

```
(NETGEAR Switch) (Interface 1/0/1-1/0/10)#rmon collection history 1 buckets 10 interval
30 owner myOwner
```

Error: 'rmon collection history' is not supported on range of interfaces.

no rmon collection history

This command will delete the history control group entry with the specified index number.

Format `no rmon collection history index-number`

Mode Interface Config

Command example:

(NETGEAR Switch) (Interface 1/0/1-1/0/10)# no rmon collection history 1

show rmon alarm | alarms

M4250

M4350

This command displays all entries in the RMON alarm table or an entry for an alarm index.

Format `show rmon {alarm alarm-index | alarms}`

Mode Privileged Exec

Term	Description
Alarm Index	An index that uniquely identifies an entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device. The range is 1 to 65535.
Alarm Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
Alarm Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.
Alarm Absolute Value	The value of the statistic during the last sampling period. This object is a read-only, 32-bit signed value.
Alarm Rising Threshold	The rising threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
Alarm Rising Event Index	The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
Alarm Falling Threshold	The falling threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
Alarm Falling Event Index	The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.
Alarm Startup Alarm	The alarm that may be sent. Possible values are rising, falling or both rising-falling. The default is rising-falling.
Alarm Owner	The owner string associated with the alarm entry. The default is monitorAlarm.

Command example:

```
(NETGEAR Switch) #show rmon alarms
```

Index	OID	Owner
1	alarmInterval.1	MibBrowser
2	alarmInterval.1	MibBrowser

Command example:

```
(NETGEAR Switch) #show rmon alarm 1
```

```
Alarm 1
-----
OID: alarmInterval.1
Last Sample Value: 1
Interval: 1
Sample Type: absolute
Startup Alarm: rising-falling
Rising Threshold: 1
Falling Threshold: 1
Rising Event: 1
Falling Event: 2
Owner: MibBrowser
```

show rmon collection history**M4250****M4350**

This command displays the entries in the RMON history control table.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show rmon collection history [interfaces <i>unit/slot/port</i>]</code>
Mode	Privileged Exec

Fully Managed Switches M4250 and M4350 Series

Term	Description
History Control Index	An index that uniquely identifies an entry in the historyControl table. Each such entry defines a set of samples at a particular interval for an interface on the device. The range is 1 to 65535.
History Control Data Source	The source interface for which historical data is collected.
History Control Buckets Requested	The requested number of discrete time intervals over which data is to be saved. The range is 1 to 65535. The default is 50.
History Control Buckets Granted	The number of discrete sampling intervals over which data shall be saved. This object is read-only. The default is 10.
History Control Interval	The interval in seconds over which the data is sampled. The range is 1 to 3600. The default is 1800.
History Control Owner	The owner string associated with the history control entry. The default is monitorHistoryControl.

Command example:

```
(NETGEAR Switch) #show rmon collection history
```

Index	Interface	Interval	Requested Samples	Granted Samples	Owner
1	1/0/1	30	10	10	myowner
2	1/0/1	1800	50	10	monitorHistoryControl
3	1/0/2	30	50	10	monitorHistoryControl
4	1/0/2	1800	50	10	monitorHistoryControl
5	1/0/3	30	50	10	monitorHistoryControl
6	1/0/3	1800	50	10	monitorHistoryControl
7	1/0/4	30	50	10	monitorHistoryControl
8	1/0/4	1800	50	10	monitorHistoryControl
9	1/0/5	30	50	10	monitorHistoryControl
10	1/0/5	1800	50	10	monitorHistoryControl
11	1/0/6	30	50	10	monitorHistoryControl
12	1/0/6	1800	50	10	monitorHistoryControl
13	1/0/7	30	50	10	monitorHistoryControl
14	1/0/7	1800	50	10	monitorHistoryControl
15	1/0/8	30	50	10	monitorHistoryControl
16	1/0/8	1800	50	10	monitorHistoryControl
17	1/0/9	30	50	10	monitorHistoryControl
18	1/0/9	1800	50	10	monitorHistoryControl
19	1/0/10	30	50	10	monitorHistoryControl

--More-- or (q)uit

Command example:

```
(NETGEAR Switch) #show rmon collection history interfaces 1/0/1
```

Index	Interface	Interval	Requested Samples	Granted Samples	Owner

1	1/0/1	30	10	10	myowner
2	1/0/1	1800	50	10	monitorHistoryControl

show rmon events**M4250****M4350**

This command displays the entries in the RMON event table.

Format show rmon events

Mode Privileged Exec

Term	Description
Event Index	An index that uniquely identifies an entry in the event table. Each such entry defines one event that is to be generated when the appropriate conditions occur. The range is 1 to 65535.
Event Description	A comment describing the event entry. The default is alarmEvent.
Event Type	The type of notification that the probe makes about the event. Possible values are None, Log, SNMP Trap, Log and SNMP Trap. The default is None.
Event Owner	Owner string associated with the entry. The default is monitorEvent.
Event Community	The SNMP community specific by this octet string which is used to send an SNMP trap. The default is public.
Owner	Event owner. The owner string associated with the entry.
Last time sent	The last time over which a log or a SNMP trap message is generated.

Command example:

```
(NETGEAR Switch) # show rmon events
```

Index	Description	Type	Community	Owner	Last time sent

1	test	log	public	MIB	0 days 0 h:0 m:0 s

show rmon history

M4250

M4350

This command displays the specified entry in the RMON history table.

Format	<code>show rmon history index {errors high-capacity other throughput} [period seconds]</code>
Mode	Privileged Exec
Term	Description
History Control Index	An index that uniquely identifies an entry in the historyControl table. Each such entry defines a set of samples at a particular interval for an interface on the device. The range is 1 to 65535.
History Control Data Source	The source interface for which historical data is collected.
History Control Buckets Requested	The requested number of discrete time intervals over which data is to be saved. The range is 1 to 65535. The default is 50.
History Control Buckets Granted	The number of discrete sampling intervals over which data shall be saved. This object is read-only. The default is 10.
History Control Interval	The interval in seconds over which the data is sampled. The range is 1 to 3600. The default is 1800.
History Control Owner	The owner string associated with the history control entry. The default is monitorHistoryControl.
Maximum Table Size	Maximum number of entries that the history table can hold.
Time	Time at which the sample is collected, displayed as period seconds.
CRC Align	Number of CRC align errors.
Undersize Packets	Total number of undersize packets. Packets are less than 64 octets long (excluding framing bits, including FCS octets).
Oversize Packets	Total number of oversize packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets).
Fragments	Total number of fragment packets. Packets are not an integral number of octets in length or had a bad Frame Check Sequence (FCS), and are less than 64 octets in length (excluding framing bits, including FCS octets).
Jabbers	Total number of jabber packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets), and are not an integral number of octets in length or had a bad Frame Check Sequence (FCS).
Octets	Total number of octets received on the interface.
Packets	Total number of packets received (including error packets) on the interface.
Broadcast	Total number of good Broadcast packets received on the interface.
Multicast	Total number of good Multicast packets received on the interface.

Fully Managed Switches M4250 and M4350 Series

Term	Description
Util	Port utilization of the interface associated with the history index specified.
Dropped Collisions	Total number of dropped collisions.

Command example:

```
(NETGEAR Switch) #show rmon history 1 errors
```

```
Sample set: 1   Owner: myowner
Interface: 1/0/1   Interval: 30
Requested Samples: 10   Granted Samples: 10
Maximum table size: 1758
```

Time	CRC Align	Undersize	Oversize	Fragments	Jabbers
-----	-----	-----	-----	-----	-----
Jan 01 1970 21:41:43	0	0	0	0	0
Jan 01 1970 21:42:14	0	0	0	0	0
Jan 01 1970 21:42:44	0	0	0	0	0
Jan 01 1970 21:43:14	0	0	0	0	0
Jan 01 1970 21:43:44	0	0	0	0	0
Jan 01 1970 21:44:14	0	0	0	0	0
Jan 01 1970 21:44:45	0	0	0	0	0
Jan 01 1970 21:45:15	0	0	0	0	0
Jan 01 1970 21:45:45	0	0	0	0	0
Jan 01 1970 21:46:15	0	0	0	0	0

Command example:

```
(NETGEAR Switch) #show rmon history 1 throughput
```

```
Sample set: 1   Owner: myowner
Interface: 1/0/1   Interval: 30
Requested Samples: 10   Granted Samples: 10
Maximum table size: 1758
```

Time	Octets	Packets	Broadcast	Multicast	Util
-----	-----	-----	-----	-----	-----
Jan 01 1970 21:41:43	0	0	0	0	1
Jan 01 1970 21:42:14	0	0	0	0	1
Jan 01 1970 21:42:44	0	0	0	0	1
Jan 01 1970 21:43:14	0	0	0	0	1
Jan 01 1970 21:43:44	0	0	0	0	1
Jan 01 1970 21:44:14	0	0	0	0	1
Jan 01 1970 21:44:45	0	0	0	0	1
Jan 01 1970 21:45:15	0	0	0	0	1
Jan 01 1970 21:45:45	0	0	0	0	1

Fully Managed Switches M4250 and M4350 Series

```
Jan 01 1970 21:46:15 0          0          0          0          1
```

Command example:

```
(NETGEAR Switch) #show rmon history 1 other
```

```
Sample set: 1   Owner: myowner
Interface: 1/0/1   Interval: 30
Requested Samples: 10   Granted Samples: 10
Maximum table size: 1758
```

Time	Dropped	Collisions
-----	-----	-----
Jan 01 1970 21:41:43 0	0	0
Jan 01 1970 21:42:14 0	0	0
Jan 01 1970 21:42:44 0	0	0
Jan 01 1970 21:43:14 0	0	0
Jan 01 1970 21:43:44 0	0	0
Jan 01 1970 21:44:14 0	0	0
Jan 01 1970 21:44:45 0	0	0
Jan 01 1970 21:45:15 0	0	0
Jan 01 1970 21:45:45 0	0	0
Jan 01 1970 21:46:15 0	0	0

show rmon log

M4250

M4350

This command displays the entries in the RMON log table.

Format	show rmon log [<i>event-index</i>]

Mode	Privileged Exec

Term	Description
Maximum table size	Maximum number of entries that the log table can hold.
Event	Event index for which the log is generated.
Description	A comment describing the event entry for which the log is generated.
Time	Time at which the event is generated.

Command example:

```
(NETGEAR Switch) #show rmon log
```

```
Event      Description                               Time
-----
```

Command example:

```
(NETGEAR Switch) #show rmon log 1
```

```
Maximum table size: 10
```

```
Event      Description                               Time
-----
```

show rmon statistics interfaces**M4250****M4350**

This command displays the RMON statistics for an interface.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

```
Format      show rmon statistics interfaces unit/slot/port
```

```
Mode        Privileged Exec
```

Term	Description
Port	The interface in the unit/slot/port format
Dropped	Total number of dropped events on the interface.
Octets	Total number of octets received on the interface.
Packets	Total number of packets received (including error packets) on the interface.
Broadcast	Total number of good broadcast packets received on the interface.
Multicast	Total number of good multicast packets received on the interface.
CRC Align Errors	Total number of packets received have a length (excluding framing bits, including FCS octets) of between 64 and 1518 octets inclusive.
Collisions	Total number of collisions on the interface.

Fully Managed Switches M4250 and M4350 Series

Term	Description
Undersize Pkts	Total number of undersize packets. Packets are less than 64 octets long (excluding framing bits, including FCS octets).
Oversize Pkts	Total number of oversize packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets).
Fragments	Total number of fragment packets. Packets are not an integral number of octets in length or had a bad Frame Check Sequence (FCS), and are less than 64 octets in length (excluding framing bits, including FCS octets).
Jabbers	Total number of jabber packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets), and are not an integral number of octets in length or had a bad Frame Check Sequence (FCS).
64 Octets	Total number of packets which are 64 octets in length (excluding framing bits, including FCS octets).
65-127 Octets	Total number of packets which are between 65 and 127 octets in length (excluding framing bits, including FCS octets).
128-255 Octets	Total number of packets which are between 128 and 255 octets in length (excluding framing bits, including FCS octets).
256-511 Octets	Total number of packets which are between 256 and 511 octets in length (excluding framing bits, including FCS octets).
512-1023 Octets	Total number of packets which are between 512 and 1023 octets in length (excluding framing bits, including FCS octets).
1024-1518 Octets	Total number of packets which are between 1024 and 1518 octets in length (excluding framing bits, including FCS octets).
HC Overflow Pkts	Total number of HC overflow packets.
HC Overflow Octets	Total number of HC overflow octets.
HC Overflow Pkts 64 Octets	Total number of HC overflow packets which are 64 octets in length
HC Overflow Pkts 65 - 127 Octets	Total number of HC overflow packets which are between 65 and 127 octets in length.
HC Overflow Pkts 128 - 255 Octets	Total number of HC overflow packets which are between 128 and 255 octets in length.
HC Overflow Pkts 256 - 511 Octets	Total number of HC overflow packets which are between 256 and 511 octets in length.
HC Overflow Pkts 512 - 1023 Octets	Total number of HC overflow packets which are between 512 and 1023 octets in length.
HC Overflow Pkts 1024 - 1518 Octets	Total number of HC overflow packets which are between 1024 and 1518 octets in length.

Command example:

```
(NETGEAR Switch) # show rmon statistics interfaces 1/0/1
Port: 1/0/1
Dropped: 0
Octets: 0  Packets: 0
Broadcast: 0  Multicast: 0
CRC Align Errors: 0  Collisions: 0
Undersize Pkts: 0  Oversize Pkts: 0
Fragments: 0  Jabbers: 0
64 Octets: 0  65 - 127 Octets: 0
128 - 255 Octets: 0  256 - 511 Octets: 0
512 - 1023 Octets: 0  1024 - 1518 Octets: 0
HC Overflow Pkts: 0  HC Pkts: 0
HC Overflow Octets: 0  HC Octets: 0
HC Overflow Pkts 64 Octets: 0  HC Pkts 64 Octets: 0
HC Overflow Pkts 65 - 127 Octets: 0  HC Pkts 65 - 127 Octets: 0
HC Overflow Pkts 128 - 255 Octets: 0  HC Pkts 128 - 255 Octets: 0
HC Overflow Pkts 256 - 511 Octets: 0  HC Pkts 256 - 511 Octets: 0
HC Overflow Pkts 512 - 1023 Octets: 0  HC Pkts 512 - 1023 Octets: 0
HC Overflow Pkts 1024 - 1518 Octets: 0  HC Pkts 1024 - 1518 Octets: 0
```

show rmon hcalarms**M4250****M4350**

This command displays all entries or a specific entry in the RMON high-capacity alarm table.

Format	<code>show rmon {hcalarms hcalarm <i>alarm-index</i>}</code>
Mode	Privileged Exec
Term	Description
High Capacity Alarm Index	An arbitrary integer index value used to uniquely identify the high capacity alarm entry. The range is 1 to 65535.
High Capacity Alarm Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
High Capacity Alarm Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.
High Capacity Alarm Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds. Possible types are Absolute Value or Delta Value. The default is Absolute Value.

Fully Managed Switches M4250 and M4350 Series

Term	Description
High Capacity Alarm Absolute Value	The absolute value (that is, the unsigned value) of the hcAlarmVariable statistic during the last sampling period. The value during the current sampling period is not made available until the period is complete. This object is a 64-bit unsigned value that is Read-Only.
High Capacity Alarm Absolute Alarm Status	This object indicates the validity and sign of the data for the high capacity alarm absolute value object (hcAlarmAbsValueobject). Possible status types are valueNotAvailable, valuePositive, or valueNegative. The default is valueNotAvailable.
High Capacity Alarm Startup Alarm	High capacity alarm startup alarm that may be sent. Possible values are rising, falling, or rising-falling. The default is rising-falling.
High Capacity Alarm Rising-Threshold Absolute Value Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
High Capacity Alarm Rising-Threshold Absolute Value High	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
High Capacity Alarm Rising-Threshold Value Status	This object indicates the sign of the data for the rising threshold, as defined by the objects hcAlarmRisingThresAbsValueLow and hcAlarmRisingThresAbsValueHigh. Possible values are valueNotAvailable, valuePositive, or valueNegative. The default is valuePositive.
High Capacity Alarm Falling-Threshold Absolute Value Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
High Capacity Alarm Falling-Threshold Absolute Value High	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
High Capacity Alarm Falling-Threshold Value Status	This object indicates the sign of the data for the falling threshold, as defined by the objects hcAlarmFallingThresAbsValueLow and hcAlarmFallingThresAbsValueHigh. Possible values are valueNotAvailable, valuePositive, or valueNegative. The default is valuePositive.
High Capacity Alarm Rising Event Index	The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
High Capacity Alarm Falling Event Index	The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.
High Capacity Alarm Failed Attempts	The number of times the associated hcAlarmVariable instance was polled on behalf of this hcAlarmEntry (while in the active state) and the value was not available. This object is a 32-bit counter value that is read-only.
High Capacity Alarm Owner	The owner string associated with the alarm entry. The default is monitorHCArm.
High Capacity Alarm Storage Type	The type of non-volatile storage configured for this entry. This object is read-only. The default is volatile.

Command example:

```
(NETGEAR Switch) #show rmon hcalarms
```

Index	OID	Owner
1	alarmInterval.1	MibBrowser
2	alarmInterval.1	MibBrowser

Command example:

```
(NETGEAR Switch) #show rmon hcalarm 1
```

```
Alarm 1
-----
OID: alarmInterval.1
Last Sample Value: 1
Interval: 1
Sample Type: absolute
Startup Alarm: rising-falling
Rising Threshold High: 0
Rising Threshold Low: 1
Rising Threshold Status: Positive
Falling Threshold High: 0
Falling Threshold Low: 1
Falling Threshold Status: Positive
Rising Event: 1
Falling Event: 2
Startup Alarm: Rising-Falling
Owner: MibBrowser
```

Statistics Application Commands

The statistics application gives you the ability to query for statistics on port utilization, flow-based and packet reception on programmable time slots. The statistics application collects the statistics at a configurable time range. You can specify the port number(s) or a range of ports for statistics to be displayed. The configured time range applies to all ports. Detailed statistics are collected between a specified time range in date and time format. You can define the time range as having an absolute time entry and/or a periodic time. For example, you can specify the statistics to be collected and displayed between 9:00 12 NOV 2011 (START) and 21:00 12 NOV 2012 (END) or schedule it on every Mon, Wed, and Fri 9:00 (START) to 21:00 (END).

You can receive the statistics in the following ways:

- User requests through the CLI for a set of counters.
- Configuring the device to display statistics using syslog or email alert. The syslog or email alert messages are sent by the statistics application at END time.

You can configure the device to display statistics on the console. The collected statistics are presented on the console at END time.

stats group (Global Config)

M4250

M4350

This command creates a new group with the specified ID and configures the time range and the reporting mechanism for that group. You can either configure a group ID or enter a keyword. You can configure multiple optional reporting methods.

Format	stats group {group-id congestion port-utilization received received-errors received-transmitted transmitted transmitted-errors} timerange time-range name reporting [reporting-method]
Mode	Global Config
Parameter	Description
group ID, name	Name of the group of statistics or its identifier to apply. The range is: • 1. received • 2. received-errors • 3. transmitted • 4. transmitted-errors • 5. received-transmitted • 6. port-utilization • 7. congestion The default is None.
time-range name	Name of the time range for the group or the flow-based rule. The range is 1 to 31 alphanumeric characters. The default is None.
reporting method	Report the statistics to the configured method. You can select one or multiple methods: • none (the default) • console • syslog • e-mail

Command example:

```
(NETGEAR Switch) (Config)# stats group received timerange test reporting console email
syslog
(NETGEAR Switch) (Config)# stats group received-errors timerange test reporting email
syslog
```

```
(NETGEAR Switch) (Config)# stats group received-    transmitted timerange test reporting
none
```

no stats group

This command deletes the configured group.

Format	no stats group [<i>group-id</i> <i>name</i>]
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config)# no stats group received
(NETGEAR Switch) (Config)# no stats group received-errors
(NETGEAR Switch) (Config)# no stats group received-transmitted
```

stats flow-based (Global Config)

M4250

M4350

This command configures flow based statistics rules for the specified parameters over the specified time range. You can configure multiple parameters. Only an IPv4 address is allowed as source and destination IP address

Format	stats flow-based <i>rule-id</i> <i>timerange</i> <i>time-range-name</i> [{ <i>srcip ip-address</i> } { <i>dstip ip-address</i> } { <i>srcmac mac-address</i> } { <i>dstmac mac-address</i> } { <i>srctcpport portid</i> } { <i>dsttcpport portid</i> } { <i>srcudpport portid</i> } { <i>dstudpport portid</i> }]
Mode	Global Config

Parameter	Description
rule ID	The flow-based rule ID. The range is 1 to 16. The default is None.
time range name	Name of the time range for the group or the flow-based rule. The range is 1 to 31 alphanumeric characters. The default is None.
srcip ip-address	The source IP address.
dstip ip-address	The destination IP address.
srcmac mac-address	The source MAC address.
dstmac mac-address	The destination MAC address.
srctcpport portid	The source TCP port number.
dsttcpport portid	The destination TCP port number.

Parameter	Description
srcudpport portid	The source UDP port number.
dstudpport portid	The destination UDP port number.

Command example:

```
(NETGEAR Switch) (Config)#stats flow-based 1 timerange test srcip 1.1.1.1 dstip 2.2.2.2
srcmac 1234 dstmac 1234 srctcport 123 dsttcport 123 srcudpport 123 dstudpport 123
```

```
(NETGEAR Switch) (Config)#stats flow-based 2 timerange test srcip 1.1.1.1 dstip 2.2.2.2
srctcport 123 dsttcport 123 srcudpport 123 dstudpport 123
```

no stats flow-based

This command deletes flow-based statistics.

Format	stats flow-based <i>rule-id</i>
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config)# no stats flow-based 1
```

```
(NETGEAR Switch) (Config)# no stats flow-based 2
```

stats flow-based reporting

M4250

M4350

This command configures the reporting mechanism for all the flow-based rules configured on the system. There is no per flow-based rule reporting mechanism. Setting the reporting method as **none** resets all the reporting methods. You can select one or multiple methods:

- none (the default)
- console
- syslog
- e-mail.

Format	stats flow-based reporting <i>reporting-method</i>
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config)# stats flow-based reporting console email syslog
```

```
(NETGEAR Switch) (Config)# stats flow-based reporting email syslog
```

```
(NETGEAR Switch) (Config)# stats flow-based reporting none
```

stats group (Interface Config)

M4250

M4350

This command applies the group specified on an interface or interface range.

Format	stats group { <i>group-id</i> congestion port-utilization received received-errors received-transmitted transmitted transmitted-errors}
Mode	Interface Config

Parameter	Description
group ID, name	Name of the group of statistics or its identifier to apply on the interface. The range is: 1. received 2. received-errors 3. transmitted 4. transmitted-errors 5. received-transmitted 6. port-utilization 7. congestion The default is None.

Command example:

```
(NETGEAR Switch) (Interface 1/0/1-1/0/10)# stats group 1
(NETGEAR Switch) (Interface 1/0/1-1/0/10)# stats group 2
```

no stats group

This command deletes the interface or interface range from the specified group.

Format	no stats group [<i>group-id</i> <i>name</i>]
Mode	Interface Config

Command example: .

```
(NETGEAR Switch) (Interface 1/0/1-1/0/10)# no stats group 1
(NETGEAR Switch) (Interface 1/0/1-1/0/10)# no stats group 2
```

stats flow-based (Interface Config)

M4250**M4350**

This command applies the flow-based rule specified by the ID on an interface or interface-range.

Format	<code>stats flow-based rule-id</code>
Mode	Interface Config
Parameter	Description
rule-id	The unique identifier for the flow-based rule.

Command example:

```
(NETGEAR Switch) (Interface 1/0/1-1/0/10)# stats flow-based 1
(NETGEAR Switch) (Interface 1/0/1-1/0/10)# stats flow-based 2
```

no stats flow-based

This command deletes the interface or interface-range from the flow-based rule specified.

Format	<code>no stats flow-based rule-id</code>
Mode	Interface Config

Command example:

```
(NETGEAR Switch) (Interface 1/0/1-1/0/10)# no stats flow-based 1
(NETGEAR Switch) (Interface 1/0/1-1/0/10)# no stats flow-based 2
```

show stats group

M4250**M4350**

This command displays the configured time range and the interface list for the group specified and shows collected statistics for the specified time-range name on the interface list after the time-range expiry.

Format	<code>show {group-id congestion port-utilization received received-errors received-transmitted transmitted transmitted-errors}</code>
Mode	Privileged EXEC

Parameter	Description
group ID, name	Name of the group of statistics or its identifier to apply. The range is: 1. received 2. received-errors 3. transmitted 4. transmitted-errors 5. received-transmitted 6. port-utilization 7. congestion The default is None.

Command example:

```
(NETGEAR Switch) #show stats group received
```

```
Group: received
```

```
Time Range: test
```

```
Interface List
```

```
-----
```

```
1/0/2, 1/0/4, lag 1
```

Counter ID	Interface	Counter Value
-----	-----	-----
Rx Total	1/0/2	951600
Rx Total	1/0/4	304512
Rx Total	lag 1	0
Rx 64	1/0/2	0
Rx 64	1/0/4	4758
Rx 64	lag 1	0
Rx 65to128	1/0/2	0
Rx 65to128	1/0/4	0
Rx 65to128	lag 1	0
Rx 128to255	1/0/2	4758
Rx 128to255	1/0/4	0
Rx 128to255	lag 1	0
Rx 256to511	1/0/2	0

Command example:

```
(NETGEAR Switch) #show stats group port-utilization
```

```
Group: port-utilization
```

```
Time Range: test
```

```
Interface List
```

```
-----
```

```
1/0/2, 1/0/4, lag 1
```

```
Interface Utilization (%)
```



```

-----
1/0/2      0
1/0/4      0
lag 1      0

```

show stats flow-based

M4250

M4350

This command displays the configured time range, flow-based rule parameters, and the interface list for the flow specified.

Format show stats flow-based [*rule-id* | all]

Mode Privileged EXEC

Parameter	Description

rule-id	The unique identifier for the flow-based rule.

Command example:

```
(NETGEAR Switch) #show stats flow-based all
```

```

Flow based rule Id..... 1
Time Range..... test
Source IP..... 1.1.1.1
Source MAC..... 1234
Source TCP Port..... 123
Source UDP Port..... 123
Destination IP..... 2.2.2.2
Destination MAC..... 1234
Destination TCP Port..... 123
Destination UDP Port..... 123
Interface List
-----
1/0/1 - 1/0/2

```

Interface	Hit Count

1/0/1	100
1/0/2	0

```

Flow based rule Id..... 2
Time Range..... test
Source IP..... 1.1.1.1
Source TCP Port..... 123

```

Fully Managed Switches M4250 and M4350 Series

```
Source UDP Port..... 123
Destination IP..... 2.2.2.2
Destination TCP Port..... 123
Destination UDP Port..... 123
```

Interface List

1/0/1 - 1/0/2

Interface	Hit Count

1/0/1	100

1/0/2	0

Command example:

```
(NETGEAR Switch) #show stats flow-based 2
```

```
Flow based rule Id..... 2
Time Range..... test
Source IP..... 1.1.1.1
Source TCP Port..... 123
Source UDP Port..... 123
Destination IP..... 2.2.2.2
Destination TCP Port..... 123
Destination UDP Port..... 123
```

Interface List

1/0/1 - 1/0/2

Interface	Hit Count

1/0/1	100

1/0/2	0

7

Switching Commands

This chapter describes the switching commands.

The Switching Commands chapter includes the following sections:

- [Port Configuration Commands](#)
- [Expandable Port Configurations](#)
- [Port Link Flap Commands](#)
- [Spanning Tree Protocol Commands](#)
- [Loop Protection Commands](#)
- [VLAN Commands](#)
- [Switch Port Commands](#)
- [Double VLAN Commands](#)
- [Private VLAN Commands](#)
- [Voice VLAN Commands](#)
- [Precision Time Protocol Commands](#)
- [Provisioning \(IEEE 802.1p\) Commands](#)
- [Asymmetric Flow Control Commands](#)
- [Protected Port Commands](#)
- [Private Group Commands](#)
- [GARP Commands](#)
- [GVRP Commands](#)
- [GMRP Commands](#)
- [Port-Based Network Access Control Commands](#)
- [Storm-Control Commands](#)
- [Link Dependency Commands](#)
- [Link Local Protocol Filtering Commands](#)
- [Port-Channel/LAG \(802.3ad\) Commands](#)
- [Port Mirroring Commands](#)
- [ERSPAN Source Switch Configuration Commands](#)

- [Static MAC Filtering Commands](#)
- [DHCP L2 Relay Agent Commands](#)
- [DHCP Client Commands](#)
- [DHCP Snooping Configuration Commands](#)
- [Dynamic ARP Inspection Commands](#)
- [ARP Guard Commands](#)
- [MVR Commands](#)
- [IGMP Snooping Configuration Commands](#)
- [IGMP Snooping Querier Commands](#)
- [MLD Snooping Commands](#)
- [MLD Snooping Querier Commands](#)
- [Port Security Commands](#)
- [LLDP \(802.1AB\) Commands](#)
- [LLDP-MED Commands](#)
- [Denial of Service Commands](#)
- [MAC Database Commands](#)
- [ISDP Commands](#)
- [Interface Error Disabling and Auto Recovery Commands](#)
- [UniDirectional Link Detection Commands](#)
- [IPv4 Device Tracking Commands](#)
- [Link Debounce Commands](#)
- [Audio Video Bridging Commands](#)
- [802.1AS Commands](#)
- [MRP Commands](#)
- [MMRP Commands](#)
- [MVRP Commands](#)
- [MSRP Commands](#)

The commands in this chapter are in one of three functional groups:

- **Show commands.** Display switch settings, statistics, and other information.
- **Configuration commands.** Configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- **Clear commands.** Clear some or all of the settings to factory defaults.

Port Configuration Commands

This section describes the commands you use to view and configure port settings.

interface (Global Config) (M4250 series switch)

M4250

This command gives you access to the Interface Config mode, which allows you to enable or modify the operation of an interface (port).

You can also specify a range of ports to configure at the same time by specifying the starting *slot/port* and ending *slot/port*, separated by a hyphen.

Format	<code>interface {slot/port slot/port-slot/port}</code>
Mode	Global Config

Command example:

The following example enters Interface Config mode for port 0/2:

```
(NETGEAR Switch) #configure
(NETGEAR Switch) (config)#interface 0/2
(NETGEAR Switch) (interface 0/2)#
```

Command example:

The following example enters Interface Config mode for ports 0/2 through 0/4:

```
(NETGEAR Switch) #configure
(NETGEAR Switch) (config)#interface 0/2-0/4
(NETGEAR Switch) (interface 0/2-0/4)#
```

interface (Global Config) (M4350 series switch)

M4350

This command gives you access to the Interface Config mode, which allows you to enable or modify the operation of an interface (port).

You can also specify a range of ports to configure at the same time by specifying the starting *unit/slot/port* and ending *unit/slot/port*, separated by a hyphen.

Format	<code>interface {unit/slot/port unit/slot/port-unit/slot/port}</code>
Mode	Global Config

Command example:

The following example enters Interface Config mode for port 1/0/1:

```
(NETGEAR Switch) #configure
(NETGEAR Switch) (config)#interface 1/0/1
(NETGEAR Switch) (interface 1/0/1)#
```

Command example:

The following example enters Interface Config mode for ports 1/0/1 through 1/0/4:

```
(NETGEAR Switch) #configure
(NETGEAR Switch) (config)#interface 1/0/1-1/0/4
(NETGEAR Switch) (interface 1/0/1-1/0/4)#
```

auto-negotiate**M4250****M4350**

This command enables automatic negotiation on a port or range of ports.

Default	enabled
Format	auto-negotiate
Mode	Interface Config

no auto-negotiate

This command disables automatic negotiation on a port. Automatic sensing is disabled when automatic negotiation is disabled.

Format	no auto-negotiate
Mode	Interface Config

auto-negotiate all**M4250****M4350**

This command enables automatic negotiation on all ports.

Default	enabled
Format	auto-negotiate all
Mode	Global Config

no auto-negotiate all

This command disables automatic negotiation on all ports.

Format	no auto-negotiate all

Mode	Global Config

description (Interface Config)

M4250

M4350

Use this command to create an alpha-numeric description of an interface or range of interfaces.

Format	description <i>description</i>

Mode	Interface Config

mtu

M4250

M4350

Use the **mtu** command to set the maximum transmission unit (MTU) size, in bytes, for frames that ingress or egress the interface. You can use the **mtu** command to configure jumbo frame support for physical and port-channel (LAG) interfaces. The MTU size is an integer between 1500 and 12227 for an M4250 series switch and between 1500 and 12266 for an M4350 series switch.

Note: To receive and process packets, the Ethernet MTU must include any extra bytes that Layer-2 headers might require. To configure the IP MTU size, which is the maximum size of the IP packet (IP Header + IP payload), see [ip mtu on page 926](#).

Default	9198 (untagged)

Format	mtu <i>size</i>

Mode	Interface Config

no mtu

This command sets the default MTU size (in bytes) for the interface.

Format	no mtu
Mode	Interface Config

shutdown (Interface Config)

M4250

M4350

This command disables a port or range of ports.

Note: You can use the **shutdown** command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default	enabled
Format	shutdown
Mode	Interface Config

no shutdown

This command enables a port.

Format	no shutdown
Mode	Interface Config

shutdown all

M4250

M4350

This command disables all ports.

You can use the **shutdown all** command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default	enabled
Format	shutdown all
Mode	Global Config

no shutdown all

This command enables all ports.

Format	no shutdown all
Mode	Global Config

speed

M4250

M4350

Use this command to enable or disable auto-negotiation and set the speed that is advertised by that port. The available speed depends on the switch model. The duplex parameter allows you to set the advertised speed for both half as well as full duplex mode.

Use the **auto** keyword to enable auto-negotiation on the port. As an option, you can set the port speed and mode, according to the available options.

Use the command without the **auto** keyword to disable auto-negotiation, in which case you must set the port speed and mode.

Half duplex mode is available only for the 10 (that is, 10 Mbps), 100 (that is, 100 Mbps), and 1000 (that is, 1000 Mbps) speeds.

Default	Auto-negotiation is enabled.
Format	speed {auto [[50G 40G 25G 10G 5G 2.5G 1000 100 10] [half-duplex full-duplex]] {50G 40G 25G 10G 5G 2.5G 1000 100 10} {half-duplex full-duplex}}
Mode	Interface Config

rgb-led mode

M4350

This command enables the RGB LED mode on a switch. When you enable this mode, you can chose a color to represent the AV network profile that is assigned to each port. The RGB LEDs display beneath each port on the front panel of the switch. By default, this setting is disabled.

Format	rgb-led mode
Mode	Global Config

Note: This command is applicable on the following switches only:
M4350-24F4X, M4350-8M2V, M4350-24M4X4V, and M4350-40F4C.

no rgb-led mode

M4350

This command disables the RGB LED mode on a switch. This is the default setting.

Format	no rgb-led mode
Mode	Global Config

Note: This command is applicable on the following switches only:
M4350-24F4X, M4350-8M2V, M4350-24M4X4V, and M4350-40F4C.

rgb-led color

M4350

Use this command to select the color you want to assign to an RGB LED for a port using a specific color code.

Format	rgb-led color <0x000000-0xffffffff>
Mode	Interface Config

To turn off the RGB LED on a port, use the color code <0x000000>.

Note: This command is applicable on the following switches only:
M4350-24F4X, M4350-8M2V, M4350-24M4X4V, and M4350-40F4C.

show port

M4250

M4350

This command displays port information.

Format	show port { <i>intf-range</i> all}
Mode	Privileged EXEC

Term	Definition
Interface	unit/slot/port
Type	If not blank, this field indicates that this port is a special type of port. The possible values are: • Mirror. The port is a monitoring port. For more information, see Port Mirroring Commands on page 694. • PC Mbr. The port is a member of a port-channel (LAG). • Probe. The port is a probe port.
Admin Mode	The Port control administration state. The port must be enabled in order for it to be allowed into the network. May be enabled or disabled. The factory default is enabled.
Admin Status	If the Admin Mode indicates that a port is disabled, this field states the reason why the port is disabled.
Physical Mode	The desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed is set from the auto-negotiation process. Note that the maximum capability of the port (full duplex -100M) is advertised. Otherwise, this object determines the port's duplex mode and transmission rate. The factory default is Auto.
Physical Status	The port speed and duplex mode.
Link Status	The Link is up or down.
Link Trap	This object determines whether or not to send a trap when link status changes. The factory default is enabled.
LACP Mode	LACP is enabled or disabled on this port.

Command example:

The following example shows output for all ports:

```
(NETGEAR Switch) #show port all
```

Admin	Physical	Physical	Link	Link	LACP	Actor		
Intf	Type	Mode	Mode	Status	Status	Trap	Mode	Timeout
-----	-----	-----	-----	-----	-----	-----	-----	-----
0/1		Enable	Auto	100 Full	Up	Enable	Enable	long
0/2		Enable	Auto	100 Full	Up	Enable	Enable	long
0/3		Enable	Auto		Down	Enable	Enable	long
0/4		Enable	Auto	100 Full	Up	Enable	Enable	long
0/5		Enable	Auto	100 Full	Up	Enable	Enable	long
0/6		Enable	Auto	100 Full	Up	Enable	Enable	long
0/7		Enable	Auto	100 Full	Up	Enable	Enable	long
0/8		Enable	Auto	100 Full	Up	Enable	Enable	long
1/1		Enable			Down	Disable	N/A	N/A
1/2		Enable			Down	Disable	N/A	N/A
1/3		Enable			Down	Disable	N/A	N/A
1/4		Enable			Down	Disable	N/A	N/A
1/5		Enable			Down	Disable	N/A	N/A
1/6		Enable			Down	Disable	N/A	N/A

Command example:

The following example shows output for a range of ports:

```
(NETGEAR Switch) #show port 0/1-1/6
```

Intf	Type	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap	LACP Mode	Actor Timeout
0/1		Enable	Auto	100 Full	Up	Enable	Enable	long
0/2		Enable	Auto	100 Full	Up	Enable	Enable	long
0/3		Enable	Auto		Down	Enable	Enable	long
0/4		Enable	Auto	100 Full	Up	Enable	Enable	long
0/5		Enable	Auto	100 Full	Up	Enable	Enable	long
0/6		Enable	Auto	100 Full	Up	Enable	Enable	long
0/7		Enable	Auto	100 Full	Up	Enable	Enable	long
0/8		Enable	Auto	100 Full	Up	Enable	Enable	long
1/1		Enable			Down	Disable	N/A	N/A
1/2		Enable			Down	Disable	N/A	N/A
1/3		Enable			Down	Disable	N/A	N/A
1/4		Enable			Down	Disable	N/A	N/A
1/5		Enable			Down	Disable	N/A	N/A
1/6		Enable			Down	Disable	N/A	N/A

show port advertise**M4250****M4350**

Use this command to display the local administrative link advertisement configuration, local operational link advertisement, and the link partner advertisement for an interface. It also displays priority resolution for speed and duplex as per 802.3 Annex 28B.3. It displays the auto-negotiation state, physical time transmitter or time receiver configuration, and link state of the port.

If the link is down, the clock is displayed as *No Link*, and a dash is displayed against the Oper Peer advertisement, and Priority Resolution. If auto-negotiation is disabled, then the admin Local Link advertisement, operational local link advertisement, operational peer advertisement, and Priority resolution fields are not displayed.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

If this command is executed without the optional *unit/slot/port* parameter, then it displays the auto-negotiation state and operational Local link advertisement for all the ports. Operational link advertisement will display speed only if it is supported by both local as well

as link partner. If auto-negotiation is disabled, then operational local link advertisement is not displayed.

Format `show port advertise [unit/slot/port]`

Mode Privileged EXEC

Command example:

The following example shows output with an optional parameter:

```
(NETGEAR switch)#show port advertise 0/1
```

```
Port: 0/1
```

```
Type: Gigabit - Level
```

```
Link State: Down
```

```
Auto Negotiation: Enabled
```

```
Clock: Auto
```

	1000f	1000h	100f	100h	10f	10h
	----	----	----	----	----	----
Admin Local Link Advertisement	no	no	yes	no	yes	no
Oper Local Link Advertisement	no	no	yes	no	yes	no
Oper Peer Advertisement	no	no	yes	yes	yes	yes
Priority Resolution	-	-	yes	-	-	-

Command example:

The following example shows output without an optional parameter:

```
(NETGEAR switch)#show port advertise
```

Port	Type	Neg	Operational Link Advertisement
-----	-----	-----	-----
0/1	Gigabit - Level	Enabled	1000f, 100f, 100h, 10f, 10h
0/2	Gigabit - Level	Enabled	1000f, 100f, 100h, 10f, 10h
0/3	Gigabit - Level	Enabled	1000f, 100f, 100h, 10f, 10h

show port description

M4250

M4350

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

This command displays the interface description. Instead of *unit/slot/port*, you can use **lag** *lag-intf-num* as an alternate way to specify the LAG interface, in which *lag-intf-num* is the LAG port number.

Format	<code>show port description [unit/slot/port lag lag-intf-num]</code>
Mode	Privileged EXEC
Term	Definition
Interface	The unit/slot/port.
ifIndex	The interface index number associated with the port.
Description	The alpha-numeric description of the interface created by the command description (Interface Config) on page 483.
MAC address	The MAC address of the port. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Bit Offset Val	The bit offset value.

Command example:

```
(NETGEAR Switch)#show port description 0/1
```

```
Interface.....0/1
ifIndex.....1
Description.....
MAC address.....00:10:18:82:0C:10
Bit Offset Val.....1
```

show port status

M4250

M4350

This command displays the status for and the state of all or specified networking ports.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show port status [unit/slot/port all lag lag-intf-num]</code>
Mode	Privileged EXEC

Term	Definition
Intf	The interface in the unit/slot/port format.
Media Type	• auto-select. The media type is automatically selected. The preferred media type is displayed. • RJ45. The media type is RJ45. • SFP. The media type is SFP.
STP Mode	Indicates whether spanning tree mode is enabled or disabled.
Physical Mode	The port speed and duplex mode. The maximum capability of the port is advertised. If autonegotiation support is enabled, the duplex mode and speed are set through the autonegotiation process.
Physical Status	The port speed and duplex mode.
Link Status	Indicates whether the link is up or down.
Loop Status	Indicates whether a loop was diagnosed.
Partner Flow Control	Indicates whether flow control at the remote end is enabled or disabled.

show RGB LED configuration

M4350

This command displays the RGB LED settings for each port. Each color displays what AV network profile is assigned to the port.

Format	<code>show rgb-led color configuration [unit/slot/port]</code>
Mode	Privileged EXEC

Note: This command is applicable on the following switches only:
M4350-24F4X, M4350-8M2V, M4350-24M4X4V, and M4350-40F4C.

show RGB LED configuration all

M4350

This command displays the RGB LED settings for all ports on the switch.

Format	<code>show rgb-led color configuration all</code>
Mode	Privileged EXEC

Note: This command is applicable on the following switches only:
M4350-24F4X, M4350-8M2V, M4350-24M4X4V, and M4350-40F4C.

debug dynamic ports

M4250

M4350

This command enables debug messages that are related to dynamic ports, that is, combo ports that are capable of detecting the media type (SFP [fiber] or Ethernet [copper]).

Format	debug dynamic ports
Mode	Privileged EXEC

no debug dynamic ports

This command disables debug messages that are related to dynamic ports, that is, combo ports that are capable of detecting the media type (SFP [fiber] or Ethernet [copper]).

Format	no debug dynamic ports
Mode	Privileged EXEC

Expandable Port Configurations

You can manage the expandable port configurations for M4350 switches with 100GBASE-X QSFP28 ports.

Expandable port configuration allows the 100G QSFP28 ports on M4350 switches to operate in breakout mode, and to function as:

- One 100G interface.
- Two 50G interfaces.
- Four 25G interfaces.

Configuring a 100G port in breakout mode enables connectivity to multiple devices using a single QSFP28 uplink port. If you configure all supported 100G ports in breakout mode, the switch provides up to 16 additional 25G interfaces (model dependent). You can manage the speed settings and configure the expanded interfaces on the Port Configuration page.

Configure Breakout Mode on the 100G Port

M4350

This command enables interface configuration:

Format	(config)# interface 1/0/43

Mode	Privilege EXEC

This command enables breakout:

Format	(interface 1/0/43)# hardware profile portmode 4x25G

Mode	Privilege EXEC

Verify Breakout Interfaces

M4350

This command checks the generated breakout interfaces:

Format	(interface 1/0/43)# show interfaces hardware profile 1/0/43

Mode	Privilege EXEC

Command example:

Interface	Mode	Operating	Expanded Interfaces
1/0/43	4x25G	4x25G	1/0/53-1/0/56
	4x25G		1/0/65-1/0/66

The “Expanded Interfaces” are the logical 25G ports created from the original 100G interface.

Configure the breakout ports for 10G operation

M4350

Enter the expanded interface range:

This command breakouts the ports from 100G into four different ports, ports 53 to 56.

Format	(config)# interface 1/0/53-1/0/56

Mode	Privilege EXEC

no auto-negotiate

This command disables the auto-negotiation feature on the port.

Format	(interface)# no auto-negotiate

Mode	Privilege EXEC

Set speed and duplex

This command sets the speed on the port.

Format	(interface)# speed 10G full duplex

Mode	Privilege EXEC

Exit the configuration mode and save:

```
# end
# save
Y
```

Port Link Flap Commands

The switch can detect the number of link-flaps that occur on all ports. If the number of link-flaps on a port exceeds a configured threshold during a configured period, the port can be placed in the D-Disable state.

By enabling auto-recovery, the port can automatically be activated again. You can also activate the port manually.

link-flap d-disable

M4250

M4350

This command enables the link-flap feature on the switch. When enabled, the switch counts the number of link flaps on a port during a configured period. If the number of link flaps on a port exceeds a configured threshold, the port is placed in the D-Disable state.

Default	enabled

Format	link-flap d-disable

Mode	Global Config

no link-flap d-disable

This command disables the link-flap feature on the switch.

Format	no link-flap d-disable

Mode	Global Config

link-flap d-disable duration

M4250**M4350**

This command configures the maximum period that a port is allowed to flap before the port is placed in the D-Disable state.

The *duration* argument can be from 3 to 200 seconds. The default is 10 seconds.

Default	10 seconds
Format	link-flap d-disable duration <i>duration</i>
Mode	Global Config

no link-flap d-disable duration

This command sets the link-flap duration to its defaults of 10 seconds.

Format	no link-flap d-disable duration
Mode	Global Config

link-flap d-disable max-count

M4250**M4350**

This command configures the maximum number of flaps that are allowed before the port is placed in the D-Disable state.

The *count* argument can be a number from 2 to 100. The default number is 5.

Default	5
Format	link-flap d-disable max-count <i>count</i>
Mode	Global Config

no link-flap d-disable max-count

This command sets the maximum number of allowed link flaps to its defaults of 5.

Format	no link-flap d-disable max-count
Mode	Global Config

show link-flap d-disable

M4250

M4350

This command displays the link-flap settings.

Format	show link-flap d-disable
Mode	Global Config
Term	Definition
Admin State	Shows whether the link-flap feature is enabled or not.
Duration (in seconds)	The maximum period that link flaps are allowed.
Max-Count	The maximum number of link flaps that are allowed.

Spanning Tree Protocol Commands

This section describes the commands you use to configure Spanning Tree Protocol (STP). STP helps prevent network loops, duplicate messages, and network instability.

Note: STP is enabled on the switch and on all ports and LAGs by default. If STP is disabled, the system does not forward BPDU messages.

spanning-tree

M4250

M4350

This command sets the spanning-tree operational mode to enabled.

Default	enabled
Format	spanning-tree
Mode	Global Config

no spanning-tree

This command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Format	no spanning-tree

Mode	Global Config

spanning-tree auto-edge

M4250

M4350

Use this command to allow the interface to become an edge port if it does not receive any BPDUs.

Default	Enabled

Format	spanning-tree auto-edge

Mode	Interface Config

no spanning-tree auto-edge

This command resets the auto-edge status of the port to the default value.

Format	no spanning-tree auto-edge

Mode	Interface Config

spanning-tree backbonefast

M4250

M4350

Use this command to enable the detection of indirect link failures and accelerate spanning tree convergence on PVSTP configured switches.

Backbonefast accelerates finding an alternate path when an indirect link to the root port goes down.

Backbonefast can be configured even if the switch is configured for MST(RSTP) or PVST mode. It only has an effect when the switch is configured for the PVST mode.

If a backbonefast-enabled switch receives an inferior BPDU from its designated switch on a root or blocked port, it sets the maximum aging time on the interfaces on which it received the inferior BPDU if there are alternate paths to the designated switch. This allows a blocked port to immediately move to the listening state where the port can be transitioned to the forwarding state in the normal manner.

On receipt of an inferior BPDU from a designated bridge, backbonefast enabled switches send a Root Link Query (RLQ) request to all non-designated ports except the port from which it received the inferior BPDU. This check validates that the switch can receive packets from the root on ports where it expects to receive BPDUs. The port from which the original inferior BPDU was received is excluded because it has already encountered a failure. Designated ports are excluded as they do not lead to the root.

On receipt of an RLQ response, if the answer is negative, the receiving port has lost connection to the root and its BPDU is immediately aged out. If all nondesignated ports have already received a negative answer, the whole bridge has lost the root and can start the STP calculation from scratch.

If the answer confirms the switch can access the root bridge on a port, it can immediately age out the port on which it initially received the inferior BPDU.

A bridge that sends an RLQ puts its bridge ID in the PDU. This ensures that it does not flood the response on designated ports.

A bridge that receives an RLQ and has connectivity to the root forwards the query toward the root through its root port.

A bridge that receives a RLQ request and does not have connectivity to the root (switch bridge ID is different from the root bridge ID in the query) or is the root bridge immediately answers the query with its root bridge ID.

RLQ responses are flooded on designated ports.

Default	NA
Format	<code>spanning-tree backbonefast</code>
Mode	Global Config

`no spanning-tree backbonefast`

This command disables backbonefast.

Note: PVRSTP embeds support for FastBackbone and FastUplink. Even if FastUplink and FastBackbone are configured, they are effective only in PVSTP mode.

Format	<code>no spanning-tree backbonefast</code>
Mode	Global Config

spanning-tree bpdupfilter

M4250**M4350**

Use this command to enable BPDU Filter on an interface or range of interfaces.

Default	Disabled
Format	spanning-tree bpdupfilter
Mode	Interface Config

no spanning-tree bpdupfilter

Use this command to disable BPDU Filter on the interface or range of interfaces.

Default	Disabled
Format	no spanning-tree bpdupfilter
Mode	Interface Config

spanning-tree bpdupfilter default

M4250**M4350**

Use this command to enable BPDU Filter on all the edge port interfaces.

Default	Disabled
Format	spanning-tree bpdupfilter default
Mode	Global Config

no spanning-tree bpdupfilter default

Use this command to disable BPDU Filter on all the edge port interfaces.

Default	Disabled
Format	no spanning-tree bpdupfilter default
Mode	Global Config

spanning-tree bpduflood

M4250**M4350**

Use this command to enable BPDU Flood on an interface or range of interfaces.

Default	Disabled
Format	spanning-tree bpduflood
Mode	Interface Config

no spanning-tree bpduflood

Use this command to disable BPDU Flood on the interface or range of interfaces.

Default	Disabled
Format	no spanning-tree bpduflood
Mode	Interface Config

spanning-tree bpduguard

M4250**M4350**

Use this command to enable BPDU Guard on the switch.

Default	Disabled
Format	spanning-tree bpduguard
Mode	Global Config

no spanning-tree bpduguard

Use this command to disable BPDU Guard on the switch.

Default	Disabled
Format	no spanning-tree bpduguard
Mode	Global Config

spanning-tree bpdumigrationcheck

M4250**M4350**

Use this command to force a transmission of rapid spanning tree (RSTP) and multiple spanning tree (MSTP) BPDUs. Specify a port to transmit BPDUs from, or use the **a11** keyword to transmit RST or MST BPDUs from all interfaces. This command forces the BPDU transmission when you execute it, so the command does not change the system configuration or have a **no** version.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>spanning-tree bpdumigrationcheck {unit/slot/port all}</code>

Mode	Global Config

spanning-tree configuration name

M4250**M4350**

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The *name* parameter is a string of up to 32 characters.

Default	base MAC address in hexadecimal notation

Format	<code>spanning-tree configuration name name</code>

Mode	Global Config

no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format	<code>no spanning-tree configuration name</code>

Mode	Global Config

spanning-tree configuration revision

M4250**M4350**

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The Configuration Identifier Revision Level is a number in the range of 0 to 65535.

Default	0
Format	<code>spanning-tree configuration revision <i>number</i></code>
Mode	Global Config

no spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value.

Format	<code>no spanning-tree configuration revision</code>
Mode	Global Config

spanning-tree cost

M4250**M4350**

Use this command to configure the external path cost for port used by a MST instance. When the `auto` keyword is used, the path cost from the port to the root bridge is automatically determined by the speed of the interface. To configure the cost manually, specify a *cost* value from 1–200000000.

Default	auto
Format	<code>spanning-tree cost {<i>cost</i> auto}</code>
Mode	Interface Config

no spanning-tree cost

This command resets the auto-edge status of the port to the default value.

Format	<code>no spanning-tree cost</code>
Mode	Interface Config

spanning-tree edgeport

M4250**M4350**

This command specifies that an interface (or range of interfaces) is an Edge Port within the common and internal spanning tree. This allows this port to transition to Forwarding State without delay.

Format	<code>spanning-tree edgeport</code>

Mode	Interface Config

no spanning-tree edgeport

This command specifies that this port is not an Edge Port within the common and internal spanning tree.

Format	<code>no spanning-tree edgeport</code>

Mode	Interface Config

spanning-tree forward-time

M4250**M4350**

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forward-time value is in seconds within a range of 4 to 30, with the value being greater than or equal to $(\text{Bridge Max Age} / 2) + 1$.

Default	15

Format	<code>spanning-tree forward-time value</code>

Mode	Global Config

no spanning-tree forward-time

This command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value.

Format	<code>no spanning-tree forward-time</code>

Mode	Global Config

spanning-tree guard

M4250

M4350

This command selects whether loop guard or root guard is enabled on an interface or range of interfaces. If neither is enabled, then the port operates in accordance with the multiple spanning tree protocol.

Default	none
Format	spanning-tree guard {none root loop}
Mode	Interface Config

no spanning-tree guard

This command disables loop guard or root guard on the interface.

Format	no spanning-tree guard
Mode	Interface Config

spanning-tree max-age

M4250

M4350

This command sets the Bridge Max Age parameter to a new value for the common and internal spanning tree. The max-age value is in seconds within a range of 6 to 40, with the value being less than or equal to $2 \times (\text{Bridge Forward Delay} - 1)$.

Default	20
Format	spanning-tree max-age value
Mode	Global Config

no spanning-tree max-age

This command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value.

Format	no spanning-tree max-age
Mode	Global Config

spanning-tree max-hops

M4250**M4350**

This command sets the Bridge Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is a range from 6 to 40.

Default	20
Format	<code>spanning-tree max-hops value</code>
Mode	Global Config

no spanning-tree max-hops

This command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value.

Format	<code>no spanning-tree max-hops</code>
Mode	Global Config

spanning-tree mode

M4250**M4350**

This command configures the global spanning tree mode. On a switch, only one mode can be enabled at a time.

When PVSTP or rapid PVSTP (PVRSTP) is enabled, MSTP/RSTP/STP is operationally disabled. To reen able MSTP/RSTP/STP, disable PVSTP/PVRSTP. By default, a NETGEAR managed switch is enabled for RSTP. In PVSTP or PVRSTP mode, BPDUs contain per-VLAN information instead of the common spanning-tree information (MST/RSTP).

PVSTP maintains independent spanning tree information about each configured VLAN. PVSTP uses IEEE 802.1Q trunking and allows a trunked VLAN to maintain blocked or forwarding state per port on a per-VLAN basis. This allows a trunk port to be forwarded on some VLANs and blocked on other VLANs.

PVRSTP is based on the IEEE 8012.1w standard. It supports fast convergence IEEE 802.1D. PVRSTP is compatible with IEEE 802.1D spanning tree. PVRSTP sends BPDUs on all ports, instead of only the root bridge sending BPDUs, and supports the discarding, learning, and forwarding states.

When the mode is changed to PVRSTP, version 0 STP BPDUs are no longer transmitted and version 2 PVRSTP BPDUs that carry per-VLAN information are transmitted on the VLANs enabled for spanning-tree. If a version 0 BPDU is seen, PVRSTP reverts to sending version 0 BPDUs.

Per VLAN Rapid Spanning Tree Protocol (PVRSTP) embeds support for PVSTP FastBackbone and FastUplink. There is no provision to enable or disable these features in PVRSTP.

Default	Disabled
Format	<code>spanning-tree mode {mst pvst rapid-pvst rstp stp}</code>
Mode	Global Config

spanning-tree mst

M4250

M4350

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree. If you specify an *mstid* parameter that corresponds to an existing multiple spanning tree instance, the configurations are done for that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the *mstid*, the configurations are done for the common and internal spanning tree instance.

If you specify the **cost** option, the command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter. You can set the path cost as a number in the range of 1 to 200000000 or **auto**. If you select **auto** the path cost value is set based on Link Speed.

If you specify the **port-priority** option, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter. The port-priority value is a number in the range of 0 to 240 in increments of 16.

Default	<code>cost—auto</code> <code>port-priority—128</code>
Format	<code>spanning-tree mst <i>mstid</i> [{cost <i>number</i> auto} port-priority <i>number</i>]</code>
Mode	Interface Config

no spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance, or in the common and internal spanning tree to the respective default values. If you specify an *mstid* parameter that corresponds to an existing multiple spanning tree instance, you are configuring that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the *mstid*, you are configuring the common and internal spanning tree instance.

If the you specify **cost**, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter, to the default value, i.e., a path cost value based on the Link Speed.

If you specify **port-priority**, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter, to the default value.

Format	<code>no spanning-tree mst <i>mstid</i> {cost port-priority}</code>

Mode	Interface Config

spanning-tree mst instance

M4250

M4350

This command adds a multiple spanning tree instance to the switch. The parameter *mstid* is a number within a range of 1 to 4094, that corresponds to the new instance ID to be added. The maximum number of multiple instances supported by the switch is 4.

Default	none

Format	<code>spanning-tree mst instance <i>mstid</i></code>

Mode	Global Config

no spanning-tree mst instance

This command removes a multiple spanning tree instance from the switch and reallocates all VLANs allocated to the deleted instance to the common and internal spanning tree. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance to be removed.

Format	<code>no spanning-tree mst instance <i>mstid</i></code>

Mode	Global Config

spanning-tree mst priority

M4250

M4350

This command sets the bridge priority for a specific multiple spanning tree instance. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance. The priority value is a number within a range of 0 to 4094.

If you specify 0 (defined as the default CIST ID) as the *mstid*, this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value is a number within a range of 0 to 4094. The twelve least significant bits are

masked according to the 802.1s specification. This causes the priority to be rounded down to the next lower valid priority.

Default	32768
Format	<code>spanning-tree mst priority <i>mstid</i> value</code>
Mode	Global Config

`no spanning-tree mst priority`

This command sets the bridge priority for a specific multiple spanning tree instance to the default value. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance.

If 0 (defined as the default CIST ID) is passed as the *mstid*, this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value.

Format	<code>no spanning-tree mst priority <i>mstid</i></code>
Mode	Global Config

`spanning-tree mst vlan`

M4250

M4350

This command adds an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are no longer associated with the common and internal spanning tree. The parameter *mstid* is a multiple spanning tree instance identifier, in the range of 0 to 4094, that corresponds to the desired existing multiple spanning tree instance. The *vlanid* can be specified as a single VLAN, a list, or a range of values. To specify a list of VLANs, enter a list of VLAN IDs in the range 1 to 4093, each separated by a comma with no spaces in between. To specify a range of VLANs, separate the beginning and ending VLAN ID with a dash (-). Spaces and zeros are not permitted. The VLAN IDs may or may not exist in the system.

Format	<code>spanning-tree mst vlan <i>mstid</i> <i>vlanid</i></code>
Mode	Global Config

`no spanning-tree mst vlan`

This command removes an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are again associated with the common and internal spanning tree.

Format	<code>no spanning-tree mst vlan <i>mstid</i> <i>vlanid</i></code>
Mode	Global Config

spanning-tree port mode

M4250

M4350

This command sets the administrative switch port state for the port to enabled for use by spanning tree.

Default	enabled
Format	spanning-tree port mode
Mode	Interface Config

no spanning-tree port mode

This command sets the administrative switch port state for the port to disabled, disabling the port for use by spanning tree.

Format	no spanning-tree port mode
Mode	Interface Config

spanning-tree port mode all

M4250

M4350

This command sets the administrative switch port state for all ports to enabled for use by spanning tree

Default	enabled
Format	spanning-tree port mode all
Mode	Global Config

no spanning-tree port mode all

This command sets the administrative switch port state for all ports to disabled, disabling the port for use by spanning tree.

Format	no spanning-tree port mode all
Mode	Global Config

spanning-tree port-priority

M4250**M4350**

Use this command to change the priority value of the port to allow the operator to select the relative importance of the port in the forwarding process. The value range is 0–240. Set this value to a lower number to prefer a port for forwarding of frames.

All LAN ports have 128 as priority value by default. PVSTP/PVRSTP puts the LAN port with the lowest LAN port number in the forwarding state and blocks other LAN ports.

The application uses the port priority value when the LAN port is configured as an edge port.

Default	enabled
Format	<code>spanning-tree port-priority value</code>
Mode	Interface Config

spanning-tree tcnguard

M4250**M4350**

Use this command to enable TCN guard on the interface. When enabled, TCN Guard restricts the interface from propagating any topology change information received through that interface.

Default	Enabled
Format	<code>spanning-tree tcnguard</code>
Mode	Interface Config

no spanning-tree tcnguard

This command resets the TCN guard status of the port to the default value.

Format	<code>no spanning-tree tcnguard</code>
Mode	Interface Config

spanning-tree transmit

M4250

M4350

This command sets the bridge transmit hold count parameter.

Default	6
Format	<code>spanning-tree transmit hold-count 1-10</code>
Mode	Global Config
Parameter	Description
hold-count	The Bridge Tx hold-count parameter. The value is an integer between 1 and 10.

no spanning-tree transmit

This command resets the bridge transmit hold count parameter to the default value.

Format	<code>no spanning-tree transmit hold-count</code>
Mode	Global Config

spanning-tree uplinkfast

M4250

M4350

Use this command to configure the rate at which gratuitous frames are sent (in packets per second) after switchover to an alternate port on PVSTP configured switches and enables uplinkfast on PVSTP switches. The range is 0-32000; the default is 150. This command has the effect of accelerating spanning-tree convergence after switchover to an alternate port.

Uplinkfast can be configured even if the switch is configured for MST(RSTP) mode, but it only has an effect when the switch is configured for PVST mode. Enabling FastUplink increases the priority by 3000. Path costs less than 3000 have an additional 3000 added when uplinkfast is enabled. This reduces the probability that the switch will become the root switch.

Uplinkfast immediately changes to an alternate root port on detecting a root port failure and changes the new root port directly to the forwarding state. A TCN is sent for this event.

After a switchover to an alternate port (new root port), uplinkfast multicasts a gratuitous frame on the new root port on behalf of each attached machine so that the rest of the network knows to use the secondary link to reach that machine.

PVRSTP embeds support for backbonefast and uplinkfast. There is no provision to enable or disable these features in PVRSTP configured switches.

Default	150
Format	<code>spanning-tree uplinkfast [max-update-rate <i>packets</i>]</code>
Mode	Global Config

no spanning-tree uplinkfast

This command disables uplinkfast on PVSTP configured switches. All switch priorities and path costs that have not been modified from their default values are set to their default values.

Format	<code>no spanning-tree uplinkfast [max-update-rate]</code>
Mode	Global Config

spanning-tree vlan

M4250

M4350

Use this command to enable spanning tree on a VLAN.

Default	None
Format	<code>spanning-tree vlan <i>vlan-list</i></code>
Mode	Global Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.

no spanning-tree vlan

Use this command to disable spanning tree on a VLAN.

Format	<code>no spanning-tree vlan <i>vlan-list</i></code>
Mode	Global Config

spanning-tree vlan cost

M4250**M4350**

Use this command to set the path cost for a port in a VLAN. The valid path cost values are in the range of 1 to 200000000 or **auto**. If **auto** is selected, the path cost value is set based on the link speed.

Default	None
Format	<code>spanning-tree vlan <i>vlan-id</i> cost {auto value}</code>
Mode	Interface Config

no spanning-tree vlan cost

This command resets the path cost for a port in a VLAN.

Format	<code>no spanning-tree vlan <i>vlan-id</i> cost</code>
Mode	Interface Config

spanning-tree vlan forward-time

M4250**M4350**

Use this command to configure the spanning tree forward delay time for a VLAN or a set of VLANs. The default is 15 seconds. Set this value to a lower number to accelerate the transition to forwarding. Take into account the end-to-end BPDU propagation delay, the maximum frame lifetime, the maximum transmission halt delay, and the message age overestimate values specific to their network when configuring this parameter.

Default	15 seconds
Format	<code>spanning-tree vlan <i>vlan-list</i> forward-time <i>seconds</i></code>
Mode	Global Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.
forward-time	The spanning tree forward delay time. The range is 4-30 seconds.

no spanning-tree vlan forward-time

This command resets the spanning tree forward delay time for a VLAN to the default value.

Format	no spanning-tree vlan <i>vlan-list</i> forward-time
Mode	Global Config

spanning-tree vlan hello-time

M4250

M4350

Use this command to configure the spanning tree hello time for a VLAN or a set of VLANs. The default is 2 seconds. Set this value to a lower number to accelerate the discovery of topology changes.

Default	2 seconds
Format	spanning-tree vlan <i>vlan-list</i> hello-time <i>seconds</i>
Mode	Global Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.
hello-time	The spanning tree forward hello time. The range is 1-10 seconds.

no spanning-tree vlan hello-time

This command resets the spanning tree hello time for a VLAN to the default value.

Format	no spanning-tree vlan <i>vlan-list</i> hello-time
Mode	Global Config

spanning-tree vlan max-age

M4250

M4350

Use this command to configure the spanning tree maximum age time for a set of VLANs. The default is 20 seconds.

Set this value to a lower number to accelerate the discovery of topology changes. The network operator must take into account the end-to-end BPDU propagation delay and message age overestimate for their specific topology when configuring this value.

The default setting of 20 seconds is suitable for a network of diameter 7, lost message value of 3, transit delay of 1, hello interval of 2 seconds, overestimate per bridge of 1 second, and a

BPDU delay of 1 second. For a network of diameter 4, a setting of 16 seconds is appropriate if all other timers remain at their default values.

Default	20 seconds
Format	<code>spanning-tree vlan <i>vlan-list</i> max-age <i>seconds</i></code>
Mode	Global Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.
max-age	The spanning tree maximum age time for a set of VLANs. The range is from 6–40 seconds.

`no spanning-tree vlan max-age`

This command resets the spanning tree maximum age time for a VLAN to the default value.

Format	<code>no spanning-tree vlan <i>vlan-list</i> max-age</code>
Mode	Global Config

`spanning-tree vlan root`

M4250

M4350

Use this command to configure 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.

The logic takes care of setting the bridge priority to a value lower (primary) or next lower (secondary) than the lowest bridge priority for the specified VLAN or a range of VLANs.

Default	32768
Format	<code>spanning-tree vlan <i>vlan-list</i> root {primary secondary}</code>
Mode	Global Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.

`no spanning-tree vlan root`

This command disables the switch from becoming the root bridge or standby root bridge.

Format	<code>no spanning-tree vlan <i>vlan-list</i> root</code>
Mode	Global Config

spanning-tree vlan priority

M4250**M4350**

Use this command to configure the bridge priority of a VLAN. The default value is 32768.

If the value configured is not among the specified values, it will be rounded off to the nearest valid value.

Default	32768
Format	<code>spanning-tree vlan <i>vlan-list</i> priority <i>priority</i></code>
Mode	Global Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.
priority	The VLAN bridge priority. Valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

no spanning-tree vlan priority

This command resets the spanning tree bridge priority for a VLAN to the default value.

Format	<code>no spanning-tree vlan <i>vlan-list</i> priority</code>
Mode	Global Config

spanning-tree vlan port-priority

M4250**M4350**

Use this command to change the VLAN port priority value of the VLAN port to allow the operator to select the relative importance of the VLAN port in the forwarding selection process when the port is configured as a point-to-point link type. Set this value to a lower number to prefer a port for forwarding of frames.

Default	None
Format	<code>spanning-tree vlan <i>vlan-id</i> port-priority <i>priority</i></code>
Mode	Interface Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.
priority	The VLAN port priority. The range is 0-255.

no spanning-tree vlan port-priority

This command resets the spanning tree port priority value of the VLAN port to the default value.

Format	no spanning-tree vlan <i>vlan-id</i> port-priority

Mode	Interface Config

show spanning-tree

M4250

M4350

This command displays spanning tree settings for the common and internal spanning tree. The following details are displayed.

Format	show spanning-tree

Mode	Privileged EXEC User EXEC

Term	Definition
Bridge Priority	Specifies the bridge priority for the Common and Internal Spanning tree (CST). The value lies between 0 and 61440. It is displayed in multiples of 4096.
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	Time in seconds.
Topology Change Count	Number of times changed.
Topology Change in Progress	Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.
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	Value of the Root Path Cost parameter for the common and internal spanning tree.
Root Port Identifier	Identifier of the port to access the Designated Root for the CST
Bridge Max Age	Derived value.
Bridge Max Hops	Bridge max-hops count for the device.
Root Port Bridge Forward Delay	Derived value.
Hello Time	Configured value of the parameter for the CST.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).

Term	Definition
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.
Regional Root Path Cost	Path Cost to the CST Regional Root.
Associated FIDs	List of forwarding database identifiers currently associated with this instance.
Associated VLANs	List of VLAN IDs currently associated with this instance.

Command example:

```
(NETGEAR switch) #show spanning-tree
```

```

Bridge Priority..... 32768
Bridge Identifier..... 80:00:00:10:18:48:FC:07
Time Since Topology Change..... 8 day 3 hr 22 min 37 sec
Topology Change Count..... 0
Topology Change in progress..... FALSE
Designated Root..... 80:00:00:10:18:48:FC:07
Root Path Cost..... 0
Root Port Identifier..... 00:00
Bridge Max Age..... 20
Bridge Max Hops..... 20
Bridge Tx Hold Count..... 6
Bridge Forwarding Delay..... 15
Hello Time..... 2
Bridge Hold Time..... 6
CST Regional Root..... 80:00:00:10:18:48:FC:07
Regional Root Path Cost..... 0

```

```

Associated FIDs          Associated VLANs
-----

```

show spanning-tree active

M4250

M4350

This command displays the spanning tree values on active ports for the modes xSTP and PV(R)STP.

Format	show spanning-tree active
Mode	Privileged EXEC User EXEC

Fully Managed Switches M4250 and M4350 Series

Command example:

```
(NETGEAR switch) #show spanning-tree active
```

```
Spanning Tree: Enabled (BPDU Flooding: Disabled) Portfast BPDU Filtering: Disabled
Mode: rstp
```

```
CST Regional Root:      80:00:00:01:85:48:F0:0F
```

```
Regional Root Path Cost: 0
```

```
##### MST 0 Vlan Mapped: 3
```

```
ROOT ID
```

```
Priority      32768
```

```
Address      00:00:EE:EE:EE:EE
```

```
This Switch is the Root.
```

```
Hello Time: 2s Max Age: 20s Forward Delay: 15s
```

```
Interfaces
```

Name	State	Prio.Nbr	Cost	Sts	Role	RestrictedPort
0/49	Enabled	128.49	2000	Forwarding	Desg	No
3/1	Enabled	96.66	5000	Forwarding	Desg	No
3/2	Enabled	96.67	5000	Forwarding	Desg	No
3/10	Enabled	96.75	0	Forwarding	Desg	No

Command example:

```
(NETGEAR switch) #show spanning-tree active
```

```
Spanning-tree enabled protocol rpvst
```

```
VLAN 1
```

```
RootID Priority      32769
```

```
Address      00:00:EE:EE:EE:EE
```

```
Cost         0
```

```
Port         This switch is the root
```

```
Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
```

```
BridgeID Priority      32769 (priority 32768 sys-id-ext 1)
```

```
Address      00:00:EE:EE:EE:EE
```

```
Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
```

```
Aging Time 300 sec
```

Interface	State	Prio.Nbr	Cost	Status	Role
0/49	Enabled	128.49	2000	Forwarding	Designated
3/1	Enabled	128.66	5000	Forwarding	Designated
3/2	Enabled	128.67	5000	Forwarding	Designated
3/10	Enabled	128.75	0	Forwarding	Designated

Fully Managed Switches M4250 and M4350 Series

```
VLAN    3
  RootID    Priority      32771
            Address      00:00:EE:EE:EE:EE
            Cost         0
            Port         This switch is the root
            Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
  BridgeID  Priority      32771 (priority 32768 sys-id-ext 3)
            Address      00:00:EE:EE:EE:EE
            Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
            Aging Time 300 sec
```

Interface	State	Prio.Nbr	Cost	Status	Role
3/1	Enabled	128.66	5000	Forwarding	Designated
3/2	Enabled	128.67	5000	Forwarding	Designated
3/10	Enabled	128.75	0	Forwarding	Designated

Command example:

```
(NETGEAR Switch) #show spanning-tree active
```

Spanning-tree enabled protocol rpvst

```
VLAN    1
  RootID    Priority      32769
            Address      00:00:EE:EE:EE:EE
            Cost         0
            Port         10(3/10 )
            Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
  BridgeID  Priority      32769 (priority 32768 sys-id-ext 1)
            Address      00:00:EE:EE:EE:EE
            Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
            Aging Time 300 sec
```

Interface	State	Prio.Nbr	Cost	Status	Role
0/49	Enabled	128.49	2000	Discarding	Alternate
3/1	Enabled	128.66	5000	Forwarding	Disabled
3/2	Enabled	128.67	5000	Forwarding	Disabled
3/10	Enabled	128.75	0	Forwarding	Root

```
VLAN    3
  RootID    Priority      32771
            Address      00:00:EE:EE:EE:EE
            Cost         0
            Port         10(3/10 )
```

Fully Managed Switches M4250 and M4350 Series

```
Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
BridgeID Priority      32771 (priority 32768 sys-id-ext 3)
Address      00:00:EE:EE:EE:EE
Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec
```

Interface	State	Prio.Nbr	Cost	Status	Role
3/1	Enabled	128.66	5000	Forwarding	Disabled
3/2	Enabled	128.67	5000	Forwarding	Disabled
3/10	Enabled	128.75	0	Forwarding	Root

show spanning-tree backbonefast

M4250

M4350

This command displays spanning tree information for backbonefast.

Format	show spanning-tree backbonefast

Mode	Privileged EXEC User EXEC

Term	Definition
Transitions via Backbonefast	The number of backbonefast transitions.
Inferior BPDUs received (all VLANs)	The number of inferior BPDUs received on all VLANs.
RLQ request PDUs received (all VLANs)	The number of root link query (RLQ) requests PDUs received on all VLANs.
RLQ response PDUs received (all VLANs)	The number of RLQ response PDUs received on all VLANs.
RLQ request PDUs sent (all VLANs)	The number of RLQ request PDUs sent on all VLANs.
RLQ response PDUs sent (all VLANs)	The number of RLQ response PDUs sent on all VLANs.

Command example:

```
(NETGEAR Switch)#show spanning-tree backbonefast
```

```
Backbonefast Statistics
```

```
-----
Transitions via Backbonefast (all VLANs)      : 0
Inferior BPDUs received (all VLANs)            : 0
RLQ request PDUs received (all VLANs)          : 0
RLQ response PDUs received (all VLANs)         : 0
RLQ request PDUs sent (all VLANs)              : 0
RLQ response PDUs sent (all VLANs)             : 0
```

show spanning-tree brief

M4250**M4350**

This command displays spanning tree settings for the bridge. The following information appears.

Format	show spanning-tree brief
Mode	Privileged EXEC User EXEC
Term	Definition
Bridge Priority	Configured value.
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.
Bridge Max Age	Configured value.
Bridge Max Hops	Bridge max-hops count for the device.
Bridge Hello Time	Configured value.
Bridge Forward Delay	Configured value.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).

Command example:

```
(NETGEAR Switch) #show spanning-tree brief
```

```
Bridge Priority..... 32768
Bridge Identifier..... 80:00:00:10:18:48:FC:07
Bridge Max Age..... 20
Bridge Max Hops..... 20
Bridge Hello Time..... 2
Bridge Forward Delay..... 15
Bridge Hold Time..... 6
```

show spanning-tree interface

M4250**M4350**

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Instead of *unit/slot/port*, you can use **lag** *lag-intf-num* as an alternate way to specify the LAG interface, in which *lag-intf-num* is the LAG port number. You can also use **all** to show the display the settings for all interfaces. The following details are displayed on execution of the command.

Format	show spanning-tree interface { <i>unit/slot/port</i> lag <i>lag-intf-num</i> all}		
Mode	Privileged EXEC User EXEC		
Term	Definition		
Hello Time	Admin hello time for this port.		
Port Mode	Enabled or disabled.		
BPDU Guard Effect	Enabled or disabled.		
Root Guard	Enabled or disabled.		
Loop Guard	Enabled or disabled.		
TCN Guard	Enable or disable the propagation of received topology change notifications and topology changes to other ports.		
BPDU Filter Mode	Enabled or disabled.		
BPDU Flood Mode	Enabled or disabled.		
Auto Edge	To enable or disable the feature that causes a port that has not seen a BPDU for edge delay time, to become an edge port and transition to forwarding faster.		
Port Up Time Since Counters Last Cleared	Time since port was reset, displayed in days, hours, minutes, and seconds.		
STP BPDUs Transmitted	Spanning Tree Protocol Bridge Protocol Data Units sent.		
STP BPDUs Received	Spanning Tree Protocol Bridge Protocol Data Units received.		
RSTP BPDUs Transmitted	Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.		
RSTP BPDUs Received	Rapid Spanning Tree Protocol Bridge Protocol Data Units received.		

Term	Definition
MSTP BPDUs Transmitted	Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.
MSTP BPDUs Received	Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

Command example:

```
(NETGEAR Switch) #show spanning-tree interface 0/1
Hello Time..... Not Configured
Port Mode..... Enabled
BPDU Guard Effect..... Disabled
Root Guard..... FALSE
Loop Guard..... FALSE
TCN Guard..... FALSE
BPDU Filter Mode..... Disabled
BPDU Flood Mode..... Disabled
Auto Edge..... TRUE
Port Up Time Since Counters Last Cleared..... 8 day 3 hr 39 min 58 sec
STP BPDUs Transmitted..... 0
STP BPDUs Received..... 0
RSTP BPDUs Transmitted..... 0
RSTP BPDUs Received..... 0
MSTP BPDUs Transmitted..... 0
MSTP BPDUs Received..... 0
```

Command example:

```
(NETGEAR Switch) #show spanning-tree interface lag 1
Hello Time..... Not Configured
Port Mode..... Enabled
BPDU Guard Effect..... Disabled
Root Guard..... FALSE
Loop Guard..... FALSE
TCN Guard..... FALSE
BPDU Filter Mode..... Disabled
BPDU Flood Mode..... Disabled
Auto Edge..... TRUE
Port Up Time Since Counters Last Cleared..... 8 day 3 hr 42 min 5 sec
STP BPDUs Transmitted..... 0
STP BPDUs Received..... 0
RSTP BPDUs Transmitted..... 0
RSTP BPDUs Received..... 0
MSTP BPDUs Transmitted..... 0
MSTP BPDUs Received..... 0
```


show spanning-tree mst detailed

M4250

M4350

This command displays the detailed settings for a specific MST instance or for all MST instances.

Format	show spanning-tree mst detailed { <i>mstid</i> all}
Mode	Privileged EXEC User EXEC
Parameter	Description
mstid	A multiple spanning tree instance identifier. The value is 0–4094.

Command example:

```
(NETGEAR Switch) #show spanning-tree mst detailed 0
```

```
MST Instance ID..... 0
MST Bridge Priority..... 32768
MST Bridge Identifier..... 80:00:00:10:18:48:FC:07
Time Since Topology Change..... 8 day 3 hr 47 min 7 sec
Topology Change Count..... 0
Topology Change in progress..... FALSE
Designated Root..... 80:00:00:10:18:48:FC:07
Root Path Cost..... 0
Root Port Identifier..... 00:00
```

```
Associated FIDs          Associated VLANs
-----
```

show spanning-tree mst port detailed

M4250

M4350

This command displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

You can also use **lag** *lag-intf-num* to specify a LAG interface, in which *lag-intf-num* is the LAG port number.

Format	<code>show spanning-tree mst port detailed mstid [unit/slot/port lag lag-intf-num]</code>
Mode	Privileged EXEC User EXEC

Term	Definition
MST Instance ID	The ID of the existing multiple spanning tree (MST) instance identifier. The value is 0–4094.
Port Identifier	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 Priority	The priority for a particular port within the selected MST instance. The port priority is displayed in multiples of 16.
Port Forwarding State	Current spanning tree state of this port.
Port Role	Each enabled MST Bridge Port receives a Port Role for each spanning tree. The port role is one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled.
Port Path Cost	Configured value of the Internal Port Path Cost parameter.
Designated Root	The Identifier of the designated root for this port.
Root Path Cost	The path cost to get to the root bridge for this instance. The root path cost is zero if the bridge is the root bridge for that instance.
Designated Bridge	Bridge Identifier of the bridge with the Designated Port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Loop Inconsistent State	The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. Loop inconsistent state maintains the port in a blocking state until a subsequent BPDU is received.
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

If you specify 0 (defined as the default CIST ID) as the *mstid*, this command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The *unit/slot/port* is the desired switch port. In this case, the following are displayed

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Port Identifier	The port identifier for this port within the CST.
Port Priority	The priority of the port within the CST.
Port Forwarding State	The forwarding state of the port within the CST.
Port Role	The role of the specified interface within the CST.
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled or not (disabled).
Port Path Cost	The configured path cost for the specified interface.
Auto-Calculate External Port Path Cost	Indicates whether auto calculation for external port path cost is enabled.
External Port Path Cost	The cost to get to the root bridge of the CIST across the boundary of the region. This means that if the port is a boundary port for an MSTP region, then the external path cost is used.
Designated Root	Identifier of the designated root for this port within the CST.
Root Path Cost	The root path cost to the LAN by the port.
Designated Bridge	The bridge containing the designated port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Topology Change Acknowledgement	Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.
Hello Time	The hello time in use for this port.
Edge Port	The configured value indicating if this port is an edge port.
Edge Port Status	The derived value of the edge port status. True if operating as an edge port; false otherwise.
Point To Point MAC Status	Derived value indicating if this port is part of a point to point link.
CST Regional Root	The regional root identifier in use for this port.
CST Internal Root Path Cost	The internal root path cost to the LAN by the designated external port.
Loop Inconsistent State	The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. Loop inconsistent state maintains the port in a blocking state until a subsequent BPDU is received.

Term	Definition
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

Command example:

The following example shows output for the command in the unit/port format:

```
(NETGEAR Switch) #show spanning-tree mst port detailed 0 0/1
```

```
Port Identifier..... 80:01
Port Priority..... 128
Port Forwarding State..... Disabled
Port Role..... Disabled
Auto-calculate Port Path Cost..... Enabled
Port Path Cost..... 0
Auto-Calculate External Port Path Cost..... Enabled
External Port Path Cost..... 0
Designated Root..... 80:00:00:10:18:48:FC:07
Root Path Cost..... 0
Designated Bridge..... 80:00:00:10:18:48:FC:07
Designated Port Identifier..... 00:00
Topology Change Acknowledge..... FALSE
Hello Time..... 2
Edge Port..... FALSE
Edge Port Status..... FALSE
Point to Point MAC Status..... TRUE
CST Regional Root..... 80:00:00:10:18:48:FC:07
CST Internal Root Path Cost..... 0
Loop Inconsistent State..... FALSE
Transitions Into Loop Inconsistent State..... 0
Transitions Out Of Loop Inconsistent State..... 0
```

Command example:

The following example shows output using a LAG interface number:

```
(NETGEAR Switch) #show spanning-tree mst port detailed 0 lag 1
```

```
Port Identifier..... 60:42
Port Priority..... 96
Port Forwarding State..... Disabled
Port Role..... Disabled
Auto-calculate Port Path Cost..... Enabled
```

```

Port Path Cost..... 0
Auto-Calculate External Port Path Cost..... Enabled
External Port Path Cost..... 0
Designated Root..... 80:00:00:10:18:48:FC:07
Root Path Cost..... 0
Designated Bridge..... 80:00:00:10:18:48:FC:07
Designated Port Identifier..... 00:00
Topology Change Acknowledge..... FALSE
Hello Time..... 2
Edge Port..... FALSE
Edge Port Status..... FALSE
Point to Point MAC Status..... TRUE
CST Regional Root..... 80:00:00:10:18:48:FC:07
CST Internal Root Path Cost..... 0
Loop Inconsistent State..... FALSE
Transitions Into Loop Inconsistent State..... 0
Transitions Out Of Loop Inconsistent State..... 0
--More-- or (q)uit

```

show spanning-tree mst port summary

M4250

M4350

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter *mstid* indicates a particular MST instance.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The keyword **a11** indicates all ports. You can also use **lag** *lag-intf-num* to specify the LAG interface, in which *lag-intf-num* is the LAG port number.

If you specify 0 (defined as the default CIST ID) as the *mstid*, the status summary displays for one or all ports within the common and internal spanning tree.

Format	<code>show spanning-tree mst port summary mstid {unit/slot/port lag lag-intf-num all}</code>
Mode	Privileged EXEC User EXEC

Term	Definition
MST Instance ID	The MST instance associated with this port.
Interface	The interface.
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.
Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.
Port Role	The role of the specified port within the spanning tree.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

Command example:

The following example shows output in the unit/port format:

```
(NETGEAR Switch) #show spanning-tree mst port summary 0 0/1
```

```
MST Instance ID..... CST
```

Interface	STP Mode	Type	STP State	Port Role	Desc
0/1	Enabled		Disabled	Disabled	

Command example:

The following example shows output using a LAG interface number:

```
(NETGEAR Switch) #show spanning-tree mst port summary 0 lag 1
```

```
MST Instance ID..... CST
```

Interface	STP Mode	Type	STP State	Port Role	Desc
3/1	Enabled		Disabled	Disabled	

show spanning-tree mst port summary active

M4250

M4350

This command displays settings for the ports within the specified multiple spanning tree instance that are active links.

Format	show spanning-tree mst port summary <i>mstid</i> active
Mode	Privileged EXEC User EXEC
Term	Definition
MST Instance ID	The ID of the existing MST instance.
Interface	The interface.
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.
Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.
Port Role	The role of the specified port within the spanning tree.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

Command example:

```
(NETGEAR Switch) #show spanning-tree mst port summary 0 active
```

Interface	STP Mode	Type	STP State	Port Role	Desc
-----	-----	-----	-----	-----	-----

show spanning-tree mst summary

M4250**M4350**

This command displays summary information about all multiple spanning tree instances in the switch.

Term	Definition
MST Instance ID List	List of multiple spanning trees IDs currently configured.
For each MSTID:	List of forwarding database identifiers associated with this instance.
Associated FIDs	List of VLAN IDs associated with this instance.
Associated VLANs	

show spanning-tree summary

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

Format	show spanning-tree summary
Mode	Privileged EXEC User EXEC

Term	Definition
Spanning Tree Adminmode	Enabled or disabled.
Spanning Tree Version	Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter.
BPDU Guard Mode	Enabled or disabled.
BPDU Filter Mode	Enabled or disabled.
Configuration Name	Identifier used to identify the configuration currently being used.
Configuration Revision Level	Identifier used to identify the configuration currently being used.
Configuration Digest Key	A generated Key used in the exchange of the BPDUs.
Configuration Format Selector	Specifies the version of the configuration format being used in the exchange of BPDUs. The default value is zero.
MST Instances	List of all multiple spanning tree instances configured on the switch.

Command example:

```
(NETGEAR Switch) #show spanning-tree summary
```

```
Spanning Tree Adminmode..... Enabled
Spanning Tree Version..... IEEE 802.1s
```



```

BPDU Guard Mode..... Disabled
BPDU Filter Mode..... Disabled
Configuration Name..... ****
Configuration Revision Level..... ****
Configuration Digest Key..... ****
Configuration Format Selector..... 0
No MST instances to display.

```

show spanning-tree uplinkfast

M4250

M4350

This command displays spanning tree information for uplinkfast.

Format	show spanning-tree uplinkfast
Mode	Privileged EXEC User EXEC
Term	Definition
Uplinkfast transitions (all VLANs)	The number of uplinkfast transitions on all VLANs.
Proxy multicast addresses transmitted (all VLANs)	The number of proxy multicast addresses transmitted on all VLANs.

Command example:

```

(NETGEAR Switch) #show spanning-tree uplinkfast
Uplinkfast is enabled.
BPDU update rate : 150 packets/sec

Uplinkfast Statistics
-----
Uplinkfast transitions (all VLANs)..... 0
Proxy multicast addresses transmitted (all VLANs).. 0

```

show spanning-tree vlan

M4250

M4350

This command displays spanning tree information per VLAN and also lists out the port roles and states along with port cost. The *vlan-list* parameter is a list of VLANs or VLAN-ranges separated by commas and with no embedded blank spaces. VLAN ranges are of the form “X-Y” where X and Y are valid VLAN identifiers and X < Y. The *vlanid* parameter corresponds to an existing VLAN ID.

Format `show spanning-tree vlan {vlanid | vlan-list}`

Mode Privileged EXEC
 User EXEC

Command example:

(NETGEAR Switch) `show spanning-tree vlan 1`

```

VLAN      1
    Spanning-tree enabled protocol rpvst
    RootID      Priority      32769
    Address      00:0C:29:D3:80:EA
    Cost         0
    Port         This switch is the root
    Hello Time 2 Sec Max Age 15 sec Forward Delay 15 sec
    BridgeID     Priority      32769 (priority 32768 sys-id-ext 1)
    Address      00:0C:29:D3:80:EA
    Hello Time 2 Sec Max Age 15 sec Forward Delay 15 sec
    Aging Time 300
Interface  Role      Sts      Cost      Prio.Nbr
-----
1/0/1     Designated Forwarding 3000      128.1
1/0/2     Designated Forwarding 3000      128.2
1/0/3     Disabled   Disabled  3000      128.3
1/0/4     Designated Forwarding 3000      128.4
1/0/5     Designated Forwarding 3000      128.5
1/0/6     Designated Forwarding 3000      128.6
1/0/7     Designated Forwarding 3000      128.7
1/0/8     Designated Forwarding 3000      128.8
0/1/1     Disabled   Disabled  3000      128.1026
0/1/2     Disabled   Disabled  3000      128.1027
0/1/3     Disabled   Disabled  3000      128.1028
0/1/4     Disabled   Disabled  3000      128.1029
0/1/5     Disabled   Disabled  3000      128.1030
0/1/6     Disabled   Disabled  3000      128.1031

```

Loop Protection Commands

This section describes the commands that you can use to configure loop protection. Loop protection detects physical and logical loops between Ethernet ports on a device. You must enable loop protection globally before you can enable it at the interface level.

keepalive

M4250

M4350

This command enables loop protection globally on the switch. As an option, you can configure the time in seconds between the transmission of keep-alive packets (that is, the transmit *interval* argument) and the maximum number of keep-alive packets (that is, the *packet-count* argument) that the switch can receive before an action is taken.

Default	Disabled Interval is 5 seconds Packet count is 1
Format	<code>keepalive [interval] [packet-count]</code>
Mode	Global Config

no keepalive

This command disables loop protection globally on the switch. This command also sets the transmit interval and packet count to the default value.

Format	<code>no keepalive</code>
Mode	Global Config

keepalive action

M4250

M4350

This command configures the action that must follow when a loop is detected on a port.

Default	Disable
Format	<code>keepalive action {log disable both}</code>
Mode	Interface Config

Parameter	Description
log	The message is logged to a buffer log but the interface is not brought down.
disable	The interface is brought down but the message is not logged.
both	The interface is brought down and the message is logged.

no keepalive action

This command returns the command to the default action of disabling an interface when a loop is detected.

Format	<code>no keepalive action</code>
Mode	Interface Config

keepalive tag

M4250

M4350

This command configures the VLAN to be used when generating the VLAN tag of the loop protection PDUs. The tag protocol identifier (TPID) is dot1q.

Default	Disabled
Format	<code>keepalive tag dot1q vlan-id</code>
Mode	Interface Config

Parameter	Description
dot1q	Uses a TPID of 0x8100.
dot1ad	Uses a TPID of 0x88A8.
<i>vlan-id</i>	The ID of the VLAN that must be used when generating the VLAN.

no keepalive tag

This command removes the VLAN-based loop protection and resets the port to port-based loop protection only.

Format	<code>no keepalive tag</code>
Mode	Interface Config

errdisable recovery cause keepalive

M4250

M4350

This command enables the autorecovery of interfaces on which a loop was detected.

Format	<code>errdisable recovery cause keepalive</code>

Mode	Global Config

no errdisable recovery cause keepalive

This command disables the autorecovery of interfaces on which a loop was detected.

Format	<code>no errdisable recovery cause keepalive</code>

Mode	Global Config

show keepalive

M4250

M4350

This command displays the global keep-alive configuration.

As an option, to display details, use the **detail** keyword followed by either a specific interface or the **all** keyword.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

For the *unit/slot/port* argument, you can also use commas to separate interfaces or use a hyphen for a range of interfaces.

Format	<code>show keepalive [detail {unit/slot/port all}]</code>

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show keepalive
Keepalive..... Enabled
Transmit interval..... 1
Max PDU Receive..... 1
```

show keepalive statistics

M4250

M4350

This command displays the keep-alive statistics for a specific interface or for all interfaces.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show keepalive statistics { <i>unit/slot/port</i> all}
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show keepalive statistics all
```

Port	Keep Alive	Loop Detected	Loop Count	Time Since Last Loop	Rx Action	Port Status
0/1	Yes	Yes	1	85	shut-down	D-Disable
0/3	Yes	No			log-shutdown	Enable

clear counters keepalive

M4250

M4350

This command clears keep-alive statistics that are associated with the interfaces, such as the number of transmitted packets, the number of received packets, and the number of loop packets.

Format	clear counters keepalive
Mode	Privileged EXEC

VLAN Commands

This section describes the commands you use to configure VLAN settings.

switchport mode auto

M4250

M4350

This command globally enables the Auto-Trunk feature. If enabled, the switch can automatically configure a port as a trunk (that is, an Auto-Trunk) with an interconnected partner device that supports the Auto-Trunk feature.

After a port or an Auto-LAG becomes an Auto-Trunk, all VLANs on the switch become part of the trunk, allowing automatic configuration of all VLANs on the switch and partner device with which the trunk is established.

Default	Enabled
Format	switchport mode auto
Mode	Global Config

no switchport mode auto

This command globally disables the Auto-Trunk feature.

Format	no switchport mode auto
Mode	Global Config

show interfaces switchport trunk

M4250

M4350

This command displays information for all interfaces on which the Auto-Trunk feature is enabled. As an option, you can display the information for a single interface only.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show interfaces switchport trunk [unit/slot/port]
Mode	Privileged EXEC

Command example:

```
(Switch)#show interfaces switchport trunk
```

```
Global Auto-Trunk Mode : Enabled
```

Intf	PVID	Allowed Vlans List	Auto-Trunk
1/0/3	1	All	Yes
1/0/15	1	All	Yes
1/0/29	1	All	Yes

Command example:

```
(Switch)#show interfaces switchport trunk 1/0/15
```

```
Global Auto-Trunk Mode : Enabled
```

Intf	PVID	Allowed Vlans List	Auto-Trunk
1/0/15	1	All	Yes

vlan database**M4250****M4350**

This command gives you access to the VLAN Config mode (also referred to as VLAN Database mode), which allows you to configure VLAN characteristics.

Format	vlan database
Mode	Privileged EXEC

vlan**M4250****M4350**

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). The VLAN number is in the range 2–4093.

Format	vlan <i>number</i>
Mode	Global Config

no vlan

This command deletes an existing VLAN. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). The VLAN number is in the range 2–4093.

Format	<code>no vlan <i>number</i></code>

Mode	VLAN Config (also referred to as VLAN Database)

vlan acceptframe

M4250**M4350**

This command sets the frame acceptance mode on an interface or range of interfaces. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. For admituntaggedonly mode, only untagged frames are accepted on this interface; tagged frames are discarded. With any option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Default	all

Format	<code>vlan acceptframe {admituntaggedonly vlanonly all}</code>

Mode	Interface Config

no vlan acceptframe

This command resets the frame acceptance mode for the interface or range of interfaces to the default value.

Format	<code>no vlan acceptframe</code>

Mode	Interface Config

vlan ingressfilter

M4250**M4350**

This command enables ingress filtering on an interface or range of interfaces. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership

of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default	Disabled
Format	<code>vlan ingressfilter</code>
Mode	Interface Config

no vlan ingressfilter

This command disables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format	<code>no vlan ingressfilter</code>
Mode	Interface Config

vlan internal allocation

M4250

M4350

Use this command to configure which VLAN IDs to use for port-based routing interfaces. When a port-based routing interface is created, an unused VLAN ID is assigned internally.

Format	<code>vlan internal allocation {base <i>vlan-id</i> policy ascending policy descending}</code>
Mode	Global Config

Parameter	Description
<i>base vlan-id</i>	The first VLAN ID to be assigned to a port-based routing interface.
<i>policy ascending</i>	VLAN IDs assigned to port-based routing interfaces start at the base and increase in value
<i>policy descending</i>	VLAN IDs assigned to port-based routing interfaces start at the base and decrease in value

no vlan internal allocation

This command disables VLAN IDs that are used for port-based routing interfaces.

Format	<code>no vlan internal allocation {base policy}</code>
Mode	Interface Config

vlan makestatic

M4250**M4350**

This command changes a dynamically created VLAN (created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. The VLAN number is in the range is 2–4093.

Format	<code>vlan makestatic <i>number</i></code>
Mode	VLAN Config (also referred to as VLAN Database)

vlan name

M4250**M4350**

This command changes the name of a VLAN. The name is an alphanumeric string of up to 32 characters, and the number is a valid VLAN identification number. The number is in the range 1–4093.

Default	VLAN ID 1 - default other VLANs - blank string
Format	<code>vlan name <i>number name</i></code>
Mode	VLAN Config (also referred to as VLAN Database)

no vlan name

This command sets the name of a VLAN to a blank string.

Format	<code>no vlan name <i>number</i></code>
Mode	VLAN Config (also referred to as VLAN Database)

vlan participation

M4250**M4350**

This command configures the degree of participation for a specific interface or range of interfaces in a VLAN. The number is a valid VLAN identification number in the range 1-4093, and the interface is a valid interface number.

Format	<code>vlan participation {exclude include auto} <i>number</i></code>
Mode	Interface Config

Participation options are:

Options	Definition
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN by GVRP and will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

no vlan participation include

This command removes the participation for a specific interface or range of interfaces in a VLAN.

Format	<code>no vlan participation include <i>number</i></code>
Mode	Interface Config

vlan participation all

M4250

M4350

This command configures the degree of participation for all interfaces in a VLAN. The number is a valid VLAN identification number in the range 1–4093.

Format	<code>vlan participation all {exclude include auto} <i>number</i></code>
Mode	Global Config

You can use the following participation options:

Participation Options	Definition
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

no vlan participation all include

This command removes the participation for all interfaces in a VLAN.

Format	<code>no vlan participation include <i>number</i></code>
Mode	Global Config

vlan port acceptframe all

M4250

M4350

This command sets the frame acceptance mode for all interfaces.

For the **all** mode, untagged frames or priority frames that enter on an interface are accepted and assigned the VLAN ID of the interface. With any of the three modes, VLAN-tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN specification.

Default	all
Format	vlan port acceptframe all {vlanonly admituntaggedonly all}
Mode	Global Config

The modes are defined as follows:

Mode	Definition
vlanonly	VLAN-only mode. Untagged frames or priority frames received on this interface are discarded.
admituntaggedonly	Admit untagged-only mode. VLAN-tagged and priority tagged frames received on this interface are discarded.
all	Admit all mode. Untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port.

no vlan port acceptframe all

This command sets the frame acceptance mode to the default mode **all**.

Format	no vlan port acceptframe all
Mode	Global Config

vlan port ingressfilter all

M4250

M4350

This command enables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default	Disabled
Format	vlan port ingressfilter all
Mode	Global Config

no vlan port ingressfilter all

This command disables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format	no vlan port ingressfilter all

Mode	Global Config

vlan port pvid all

M4250

M4350

This command changes the VLAN ID for all interfaces. The number is a valid VLAN identification number in the range 1–4093.

Default	1

Format	vlan port pvid all <i>number</i>

Mode	Global Config

no vlan port pvid all

This command sets the VLAN ID for all interfaces to 1.

Format	no vlan port pvid all

Mode	Global Config

vlan port tagging all

M4250

M4350

This command configures the tagging behavior for all interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The number is a valid VLAN identification number in the range 1–4093.

Format	vlan port tagging all <i>number</i>

Mode	Global Config

no vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The number is a valid VLAN identification number in the range 1–4093.

Format	no vlan port tagging all <i>number</i>

Mode	Global Config

vlan protocol group

M4250

M4350

This command adds a protocol-based VLAN group. The *groupid* is a unique number from 1–128 that is used to identify the group in subsequent commands.

Format	vlan protocol group <i>groupid</i>

Mode	Global Config

no vlan protocol group

This command removes a protocol-based VLAN group identified by *groupid*.

Format	no vlan protocol group <i>groupid</i>

Mode	Global Config

vlan protocol group name

M4250

M4350

This command assigns a name to a protocol-based VLAN group. The *groupname* variable can be a character string of 0 to 16 characters.

Format	vlan protocol group name <i>groupid groupname</i>

Mode	Global Config

no vlan protocol group name

This command removes the name from the group identified by *groupid*.

Format	no vlan protocol group name <i>groupid</i>

Mode	Global Config

vlan protocol group add protocol

M4250**M4350**

This command adds the protocol to the protocol-based VLAN identified by *groupid*. A group may have more than one protocol associated with it. Each interface and protocol combination can only be associated with one group. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command fails and the protocol is not added to the group. The possible values for *protocol-list* includes the keywords **ip**, **arp**, and **ipx** and hexadecimal or decimal values ranging from 0x0600 (1536) to 0xFFFF (65535). The protocol list can accept up to 16 protocols separated by a comma.

Default	none
Format	<code>vlan protocol group add protocol <i>groupid</i> <i>ethertype</i> <i>protocol-list</i></code>
Mode	Global Config

no vlan protocol group add protocol

This command removes the protocols specified in the *protocol-list* from this protocol-based VLAN group that is identified by this *groupid*.

Format	<code>no vlan protocol group add protocol <i>groupid</i> <i>ethertype</i> <i>protocol-list</i></code>
Mode	Global Config

protocol group

M4250**M4350**

This command attaches a *vlanid* to the protocol-based VLAN identified by *groupid*. A group can only be associated with one VLAN at a time, however the VLAN association can be changed.

Default	none
Format	<code>protocol group <i>groupid</i> <i>vlanid</i></code>
Mode	VLAN Config (also referred to as VLAN Database)

no protocol group

This command removes the *vlanid* from this protocol-based VLAN group that is identified by this *groupid*.

Format	no protocol group <i>groupid</i> <i>vlanid</i>

Mode	VLAN Config (also referred to as VLAN Database)

protocol vlan group

M4250

M4350

This command adds a physical interface or a range of interfaces to the protocol-based VLAN identified by *groupid*. You can associate multiple interfaces with a group, but you can only associate each interface and protocol combination with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command fails and the interface or interfaces are not added to the group.

Default	none

Format	protocol vlan group <i>groupid</i>

Mode	Interface Config

no protocol vlan group

This command removes the interface from this protocol-based VLAN group that is identified by this *groupid*.

Format	no protocol vlan group <i>groupid</i>

Mode	Interface Config

protocol vlan group all

M4250

M4350

This command adds all physical interfaces to the protocol-based VLAN identified by *groupid*. You can associate multiple interfaces with a group, but you can only associate each interface and protocol combination with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface or interfaces are not added to the group.

Default	none

Format	protocol vlan group all <i>groupid</i>

Mode	Global Config

no protocol vlan group all

This command removes all interfaces from this protocol-based VLAN group that is identified by this *groupid*.

Format	no protocol vlan group all <i>groupid</i>

Mode	Global Config

show port protocol

M4250

M4350

This command displays the protocol-based VLAN information for either the entire system, or for the indicated group.

Format	show port protocol { <i>groupid</i> all}

Mode	Privileged EXEC

Term	Definition
Group Name	The group name of an entry in the Protocol-based VLAN table.
Group ID	The group identifier of the protocol group.
VLAN	The VLAN associated with this Protocol Group.
Protocol(s)	The type of protocol(s) for this group.
Interface(s)	Lists the interface(s) that are associated with this Protocol Group.

vlan pvid

M4250

M4350

This command changes the VLAN ID on an interface or range of interfaces. The number is a valid VLAN identification number in the range 1–4093.

Default	1

Format	vlan pvid <i>number</i>

Mode	Interface Config

no vlan pvid

This command sets the VLAN ID on an interface or range of interfaces to 1.

Format	no vlan pvid

Mode	Interface Config

vlan tagging

M4250

M4350

This command configures the tagging behavior for a specific interface or range of interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The number is a valid VLAN identification number in the range 1–4093.

Format	vlan tagging <i>number</i>

Mode	Interface Config

no vlan tagging

This command configures the tagging behavior for a specific interface or range of interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The number is a valid VLAN identification number in the range 1–4093.

Format	no vlan tagging <i>number</i>

Mode	Interface Config

vlan association subnet

M4250

M4350

This command associates a VLAN to a specific IP-subnet.

Format	vlan association subnet <i>ipaddr netmask vlanid</i>

Mode	VLAN Config (also referred to as VLAN Database)

no vlan association subnet

This command removes association of a specific IP-subnet to a VLAN.

Format	no vlan association subnet <i>ipaddr netmask</i>

Mode	VLAN Config (also referred to as VLAN Database)

vlan association mac

M4250**M4350**

This command associates a MAC address to a VLAN.

Format	<code>vlan association mac <i>macaddr</i> <i>vlanid</i></code>
Mode	VLAN Config (also referred to as VLAN Database)

no vlan association mac

This command removes the association of a MAC address to a VLAN.

Format	<code>no vlan association mac <i>macaddr</i></code>
Mode	VLAN Config (also referred to as VLAN Database)

remote-span

M4250**M4350**

This command sets the VLAN as the RSPAN VLAN.

Default	None
Format	<code>remote-span</code>
Mode	VLAN Config, accessible from Global Config mode through entering vlan <i>vlan-id</i>

no remote-span

This command removes the RSPAN capability from the VLAN.

Format	<code>no remote-span</code>
Mode	VLAN Config, accessible from Global Config mode through entering vlan <i>vlan-id</i>

vlan association oui

M4250**M4350**

This command assigns a VLAN to a port, based on the MAC OUI of the incoming packet. You can define an OUI-based VLAN by configuring a VLAN that corresponds to the MAC OUI so that the switch learns the MAC address in the L2-MAC table. If the OUI matches, the ingress port becomes a member of the OUI-based VLAN. The ingress port PVID is then set to the OUI-based VLAN. When the MAC entry expires, the ingress port is removed from the OUI-based VLAN.

Format	<code>vlan association oui-value vlan-id</code>
Mode	VLAN Config

Command example:

```
(NETGEAR Switch)# vlan association oui 00:01:02 9
```

no vlan association oui

M4250**M4350**

This command deletes an OUI-based VLAN configuration.

Format	<code>no vlan association oui-value vlan-id</code>
Mode	VLAN Config

show vlan

M4250**M4350**

This command displays information about the configured private VLANs, including primary and secondary VLAN IDs, type (community, isolated, or primary) and the ports which belong to a private VLAN.

Format	<code>show vlan {vlan-id private-vlan [type]}</code>
Mode	Privileged EXEC User EXEC

Term	Definition
Primary	Primary VLAN identifier. The range of the VLAN ID is 1 to 4093.
Secondary	Secondary VLAN identifier.

Term	Definition
Type	Secondary VLAN type (community, isolated, or primary).
Ports	Ports which are associated with a private VLAN.
VLAN ID	The VLAN identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4093.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of Default. This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or Dynamic. A dynamic VLAN can be created by GVRP registration or during the 802.1X authentication process (DOT1X) if a RADIUS-assigned VLAN does not exist on the switch.
Interface	unit/slot/port. It is possible to set the parameters for all ports by using the selectors on the top line.
Current	The degree of participation of this port in this VLAN. The permissible values are: • Include - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • Exclude - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • Autodetect - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Configured	The configured degree of participation of this port in this VLAN. The permissible values are: • Include - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • Exclude - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • Autodetect - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Tagging	The tagging behavior for this port in this VLAN. • Tagged - Transmit traffic for this VLAN as tagged frames. • Untagged - Transmit traffic for this VLAN as untagged frames.

show vlan internal usage

M4250

M4350

This command displays information about the VLAN ID allocation on the switch.

Format	show vlan internal usage
Mode	Privileged EXEC User EXEC

Term	Definition
Base VLAN ID	Identifies the base VLAN ID for Internal allocation of VLANs to the routing interface.
Allocation policy	Identifies whether the system allocates VLAN IDs in ascending or descending order.

show vlan port

M4250

M4350

This command displays VLAN port information.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show vlan port {unit/slot/port all}</code>
Mode	Privileged EXEC User EXEC

Term	Definition
Interface	The selected interface.
Port VLAN ID Configured	The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. The factory default is 1.
Port VLAN ID Current	The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. The factory default is 1.
Acceptable Frame Types	The types of frames that may 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.
Ingress Filtering	May be 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.
GVRP	May be enabled or disabled.
Default Priority	The 802.1p priority assigned to tagged packets arriving on the port.

show vlan association subnet

M4250**M4350**

This command displays the VLAN associated with a specific configured IP-Address and net mask. If no IP address and net mask are specified, the VLAN associations of all the configured IP-subnets are displayed.

Format	show vlan association subnet [<i>ipaddr netmask</i>]
Mode	Privileged EXEC
Term	Definition
IP Address	The IP address assigned to each interface.
Net Mask	The subnet mask.
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN.

show vlan association mac

M4250**M4350**

This command displays the VLAN associated with a specific configured MAC address. If no MAC address is specified, the VLAN associations of all the configured MAC addresses are displayed.

Format	show vlan association mac [<i>macaddr</i>]
Mode	Privileged EXEC
Term	Definition
Mac Address	A MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN.

show auto-vlan

M4250**M4350**

This command displays information about the active Auto-VLAN sessions. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.

- For an M4350 series switch, use the argument *slot/port*.

Format	<code>show auto-vlan interface {unit/slot/port all}</code>

Mode	Privileged EXEC

show vlan association oui

M4250

M4350

This command displays summary information about OUI associations to a VLAN.

Format	<code>show vlan association oui</code>

Mode	Privileged EXEC User EXEC

Command example:

```
(NETGEAR Switch)# show vlan association oui
Maximum OUI VLAN Entries.....128
OUI VLAN Entries Currently in Use.....4
OUI VLAN ID
-----
00:01:02 2
00:02:03 3
00:03:04 4
00:04:05 5
```

Switch Port Commands

This section describes the commands used for switch port mode.

switchport mode

M4250

M4350

Use this command to configure the mode of a switch port as access, trunk, or general:

- Trunk mode.** In trunk mode, the port becomes a member of all VLANs on the switch unless specified in the allowed list in the **switchport trunk allowed vlan** command. The PVID of the port is set to the native VLAN as specified in the **switchport trunk native vlan** command. This means that trunk ports accept both tagged and untagged packets. Untagged packets are processed on the native VLAN and tagged packets are processed on the VLAN for which the ID is contained in the packet. MAC learning is performed on both tagged and untagged packets. Tagged packets that

are received with a VLAN ID of which the port is not a member are discarded and MAC learning is not performed.

The trunk ports always transmit packets untagged on a native VLAN.

- **Access mode.** In access mode, the port becomes a member of only one VLAN. The port sends and receives untagged traffic. The port can also receive tagged traffic. Ingress filtering is enabled on the port. This means that when the VLAN ID of a received packet is not identical to the access VLAN ID, the packet is discarded.
- **General mode.** In general mode, you can perform custom configuration of the VLAN membership, PVID, tagging, ingress filtering, and so on. The general mode is legacy behavior of the switch port configuration and you use legacy CLI commands to configure the port in general mode.

Default	General mode
Format	<code>switchport mode {access trunk general}</code>
Mode	Interface Config

no switchport mode

This command resets the switch port mode to its default value.

Format	<code>no switchport mode</code>
Mode	Interface Config

switchport trunk allowed vlan

M4250

M4350

Use this command to configure the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. The default is **all**.

You can modify the VLAN list by using the **add** and **remove** options and replace the VLAN list with another list by using the **all** or **except** options. If you use the **all** option, all VLANs are added to the list of allowed VLANs. The **except** option provides an exclusion list.

Default	<code>all</code>
Format	<code>switchport trunk allowed vlan {vlan-list all {add vlan-list} {remove vlan-list} {except vlan-list}}</code>
Mode	Interface Config

Parameter	Description
<code>all</code>	Specifies all VLANs from 1 to 4093. This keyword is not allowed for commands that do not permit all VLANs in the list to be set at the same time.
<code>add</code>	Adds the defined list of VLANs to those currently set instead of replacing the list.
<code>remove</code>	Removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 4093. Extended-range VLAN IDs of the form XY or X,Y,Z are valid in this command
<code>except</code>	Lists the VLANs that must be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.)
<code>vlan-list</code>	Either a single VLAN number from 1 to 4093 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

no switchport trunk allowed

This command resets the list of allowed VLANs on the trunk port to its default value.

Format	<code>no switchport trunk allowed vlan</code>
Mode	Interface Config

switchport trunk native vlan

M4250

M4350

Use this command to configure the trunk port native VLAN (PVID) parameter of the switch port. Any ingress untagged packets on the port are tagged with the value of the native VLAN. The native VLAN must be in the allowed VLAN list for tagging of received untagged packets. Otherwise, untagged packets are discarded. Packets marked with the native VLAN are transmitted untagged from the trunk port. The default ID is 1, the default VLAN.

Default	1 (default VLAN)
Format	<code>switchport trunk native vlan <i>vlan-id</i></code>
Mode	Interface Config

no switchport trunk native vlan

Use this command to reset the trunk mode native VLAN of the switch port to its default value.

Format	<code>no switchport trunk native vlan</code>
Mode	Interface Config

switchport access vlan

M4250**M4350**

Use this command to configure the VLAN on the access port. You can assign one VLAN only to the access port. The access port is member of VLAN 1 by default. You can assign the access port to a VLAN other than VLAN 1. If you remove the access VLAN on the switch, the access port becomes a member of VLAN 1. If you configure the access port as a member of a VLAN that does not exist, an error occurs and the configuration does not change.

Default	1 (default VLAN)
Format	<code>switchport access vlan <i>vlan-id</i></code>
Mode	Interface Config

no switchport access vlan

This command resets the switch port access mode VLAN to its default value.

Format	<code>no switchport access vlan</code>
Mode	Interface Config

show interface switchport

M4250**M4350**

Use this command to either display the switch port status for all interfaces.

Format	<code>show interface switchport</code>
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show interface switchport
Packets Received Without Error..... 0
Broadcast Packets Received..... 0
Packets Received With Error..... 0
Packets Transmitted Without Errors..... 16
Broadcast Packets Transmitted..... 0
Transmit Packet Errors..... 0
Packets forwarded by cpu..... 0
IP Packets received without errors..... 0
Time Since Counters Last Cleared..... 13 day 1 hr 36 min 28 sec
```

show interfaces switchport

M4250**M4350**

Use this command to either display the switch port status for all interfaces, for a specific interface or LAG, or for a specific mode (access, trunk, or general). If you select a specific interface or LAG, you can optionally specify a group ID from 0 to 2 for a protected port group.

If you select a specific mode (access, trunk, or general) but do not specify an interface for the mode, the selected mode is displayed for all interfaces.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show interfaces switchport [<i>unit/slot/port</i> [<i>group-id</i>] lag <i>lag-int-num</i> [<i>group-id</i>] {access trunk general} [<i>unit/slot/port</i>]]

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show interfaces switchport 1/0/1
Port: 1/0/1
VLAN Membership Mode: General
Access Mode VLAN: 1 (default)
General Mode PVID: 1 (default)
General Mode Ingress Filtering: Disabled
General Mode Acceptable Frame Type: Admit all
General Mode Dynamically Added VLANs:
General Mode Untagged VLANs: 1
General Mode Tagged VLANs:
General Mode Forbidden VLANs:
Trunking Mode Native VLAN: 1 (default)
Trunking Mode Native VLAN tagging: Disable
Trunking Mode VLANs Enabled: All
Protected Port: False
```

Command example:

```
(NETGEAR Switch) #show interfaces switchport access 1/0/1

Intf      PVID
-----
1/0/1     1
```

Command example:

```
(NETGEAR Switch) #show interfaces switchport trunk 1/0/6
```

Intf	PVID	Allowed Vlans List
1/0/6	1	All

Command example:

```
(NETGEAR Switch) #show interfaces switchport general 1/0/5
```

Intf	PVID	Ingress Filtering	Acceptable Frame Type	Untagged Vlans	Tagged Vlans	Forbidden Vlans	Dynamic Vlans
1/0/5	1	Enabled	Admit All	7	10-50,55	9,100-200	88,96

Command example:

```
(NETGEAR Switch) #show interfaces switchport general
```

Intf	PVID	Ingress Filtering	Acceptable Frame Type	Untagged Vlans	Tagged Vlans	Forbidden Vlans	Dynamic Vlans
1/0/1	1	Enabled	Admit All	1,4-7	30-40,55	3,100-200	88,96
1/0/2	1	Disabled	Admit All	1	30-40,55	none	none

Double VLAN Commands

This section describes the commands you use to configure double VLAN (DVLAN). Double VLAN tagging is a way to pass VLAN traffic from one customer domain to another through a Metro Core in a simple and cost effective manner. The additional tag on the traffic helps differentiate between customers in the MAN while preserving the VLAN identification of the individual customers when they enter their own IEEE 802.1Q domain.

`dvlan-tunnel ethertype`

M4250

M4350

This command configures the ethertype globally or for an specified interface. The two-byte hex ethertype is used as the first 16 bits of the DVLAN tag. The ethertype can have the

values of **802.1Q**, **vman**, or **custom**. If the ethertype has an optional value of **custom**, then it is a custom tunnel value, and ethertype must be set to a value in the range of 1 to 65535.

Default	vman
Format	<code>dvlan-tunnel ethertype {802.1Q vman custom value}</code>
Mode	Global Config Interface Config

Parameter	Description
802.1Q	Configure the ethertype as 0x8100.
custom	Configure the value of the custom tag in the range from 1 to 65535.
vman	Represents the commonly used value of 0x88A8.

`no dvlan-tunnel ethertype`

This command removes the ethertype value globally or for an interface.

Format	<code>no dvlan-tunnel ethertype</code>
Mode	Global Config Interface Config

`mode dot1q-tunnel`

M4250

M4350

This command is used to enable Double VLAN tunneling on the specified interface.

Default	Disabled
Format	<code>mode dot1q-tunnel</code>
Mode	Interface Config

`no mode dot1q-tunnel`

This command is used to disable Double VLAN tunneling on the specified interface. By default, Double VLAN tunneling is disabled.

Format	<code>no mode dot1q-tunnel</code>
Mode	Interface Config

mode dvlan-tunnel

M4250

M4350

Use this command to enable Double VLAN tunneling on the specified interface.

Note: When you use the **mode dvlan-tunnel** command on an interface, it becomes a service provider port. Ports that do not have double VLAN tunneling enabled are customer ports.

Default	Disabled
Format	mode dvlan-tunnel
Mode	Interface Config

no mode dvlan-tunnel

This command is used to disable Double VLAN tunneling on the specified interface. By default, Double VLAN tunneling is disabled.

Format	no mode dvlan-tunnel
Mode	Interface Config

show dot1q-tunnel

M4250

M4350

Use this command without the optional parameters to display all interfaces enabled for Double VLAN tunneling. Use the optional parameters to display detailed information about Double VLAN tunneling for the specified interface.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show dot1q-tunnel [interface <i>unit/slot/port</i>]
Mode	Privileged EXEC User EXEC

show dvlan-tunnel

M4250

M4350

Use this command without the optional parameters to display all interfaces enabled for Double VLAN tunneling. Use the optional parameters to display detailed information about Double VLAN tunneling for the specified interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show dvlan-tunnel [interface <i>unit/slot/port</i>]
Mode	Privileged EXEC User EXEC

Command example:

```
(NETGEAR Switch) #show dvlan-tunnel
```

```
TPIDs Configured..... 0x88a8
Default TPID..... 0x88a8
Interfaces Enabled for DVLAN Tunneling..... None
```

Command example:

```
(NETGEAR Switch) #show dvlan-tunnel interface 1/0/1
```

```
Interface Mode    EtherType
-----
1/0/1      Disable 0x88a8
```

Private VLAN Commands

This section describes the commands you use for private VLANs. Private VLANs provides Layer 2 isolation between ports that share the same broadcast domain. In other words, it allows a VLAN broadcast domain to be partitioned into smaller point-to-multipoint subdomains. The ports participating in a private VLAN can be located anywhere in the Layer 2 network.

switchport private-vlan

M4250

M4350

This command defines a private-VLAN association for an isolated or community port or a mapping for a promiscuous port.

Format	switchport private-vlan {host-association <i>primary-vlan-id</i> <i>secondary-vlan-id</i> mapping <i>primary-vlan-id</i> [add remove] <i>secondary-vlan-list</i> mapping trunk <i>primary-vlan-id</i> [add remove] <i>secondary-vlan-list</i> } trunk {native vlan <i>vlan-id</i> allowed vlan <i>vlan-list</i> }} association trunk <i>primary-vlan-id</i> <i>secondary-vlan-id</i> }
Mode	Interface Config
Parameter	Description
host-association	Defines the VLAN association for community or host ports.
mapping	Defines the private VLAN mapping for promiscuous ports.
mapping trunk	Maps the port to a primary VLAN and selected secondary VLANs.
primary-vlan-id	Primary VLAN ID of a private VLAN.
secondary-vlan-id	Secondary (isolated or community) VLAN ID of a private VLAN.
add	Associates the secondary VLAN with the primary one.
remove	Deletes the secondary VLANs from the primary VLAN association.
secondary-vlan-list	A list of secondary VLANs to be mapped to a primary VLAN.
trunk native vlan	Defines the VLAN association for untagged packets. If not configured, untagged packets are dropped.
trunk allowed vlan	Specifies the list of allowed normal VLANs on the trunk port.
association trunk	Associates a primary VLAN with a secondary VLAN (an isolated VLAN only). Multiple private VLAN pairs can be configured.

no switchport private-vlan

This command removes the private-VLAN association or mapping from the port.

Format	no switchport private-vlan {host-association mapping mapping trunk <i>primary-vlan-id</i> trunk allowed <i>vlan-list</i> trunk native vlan <i>vlan-id</i> association trunk <i>primary-vlan-id</i> <i>secondary-vlan-id</i> }
Mode	Interface Config

switchport mode private-vlan

M4250

M4350

This command configures a port as a promiscuous or host private VLAN port. Note that the properties of each mode can be configured even when the switch is not in that mode. However, they will only be applicable once the switch is in that particular mode.

Format	switchport mode private-vlan {host promiscuous trunk promiscuous trunk secondary}
Mode	Interface Config
Parameter	Description
host	Configures an interface as a private VLAN host port. It can be either isolated or community port depending on the secondary VLAN it is associated with.
promiscuous	Configures an interface as a private VLAN promiscuous port. The promiscuous ports are members of the primary VLAN.
trunk promiscuous	Configures an interface as a private VLAN promiscuous trunk port. These ports can carry traffic of several primary VLANs and normal VLANs. An endpoint connected to a promiscuous trunk port is allowed to communicate with all the endpoints within the private VLAN and also with other ports participating in normal VLANs. These ports carry the traffic of multiple primary VLANs towards the upstream router and regular VLANs. Promiscuous trunk ports are used when the number of links connected to upstream devices must be reduced while all the endpoints in a private VLAN still must be managed, in addition to carrying traffic of normal VLANs. These ports are typically used where the switches are connected to upstream devices that do not detect private VLANs.
trunk secondary	Configures an interface as a private VLAN isolated trunk port. These ports can carry traffic of several secondary VLANs and normal VLANs.

no switchport mode private-vlan

This command removes the private-VLAN association or mapping from the port.

Format	no switchport mode private-vlan
Mode	Interface Config

private-vlan

M4250

M4350

This command configures the private VLANs and configures the association between the primary private VLAN and secondary VLANs.

Format	<code>private-vlan {association [add remove] secondary-vlan-list community isolated primary}</code>
Mode	VLAN Config, accessible from Global Config mode through entering vlan <i>vlan-id</i>

Parameter	Description
association	Associates the primary and secondary VLAN.
secondary-vlan-list	A list of secondary VLANs to be mapped to a primary VLAN.
community	Designates a VLAN as a community VLAN.
isolated	Designates a VLAN as the isolated VLAN.
primary	Designates a VLAN as the primary VLAN.

no private-vlan

This command restores normal VLAN configuration.

Format	<code>no private-vlan [association]</code>
Mode	VLAN Config, accessible from Global Config mode through entering vlan <i>vlan-id</i>

Voice VLAN Commands

This section describes the commands you use for Voice VLAN. Voice VLAN enables switch ports to carry voice traffic with defined priority so as to enable separation of voice and data traffic coming onto the port. The benefits of using Voice VLAN is to ensure that the sound quality of an IP phone could be safeguarded from deteriorating when the data traffic on the port is high.

Also the inherent isolation provided by VLANs ensures that inter-VLAN traffic is under management control and that network- attached clients cannot initiate a direct attack on voice components. QoS-based on IEEE 802.1P class of service (CoS) uses classification and scheduling to sent network traffic from the switch in a predictable manner. The system uses the source MAC of the traffic traveling through the port to identify the IP phone data flow.

The switch can be configured to support voice VLAN on a port connecting to the VoIP phone. When a VLAN is associated with the voice VLAN port, then the VLAN id info is passed onto

the VoIP phone using the LLDP-MED mechanism. The voice data coming from the VoIP phone is tagged with the exchanged VLAN ID; thus, regular data arriving on the switch is assigned the default PVID of the port, and the voice traffic is received on a predefined VLAN. The two types of traffic are therefore segregated so that better service can be provided to the voice traffic.

When a dot1p priority is associated with the voice VLAN port instead of VLAN ID, the priority information is passed onto the VoIP phone using the LLDP-MED mechanism. Thus, the voice data coming from the VoIP phone is tagged with VLAN 0 and with the exchanged priority. Regular data arriving on the switch is assigned the default priority of the port (default 0), and the voice traffic is received with higher priority, thus segregating both the traffic to provide better service to the voice traffic.

The switch can be configured to override the data traffic CoS. This feature enables overriding the 802.1P priority of the data traffic packets arriving at the port enabled for voice VLAN. Thus, a rogue client that is also connected to the voice VLAN port does not deteriorate the voice traffic.

When a VLAN ID is configured on the voice VLAN port, the VLAN ID information is passed onto the VoIP phone using the LLDP-MED mechanism. The voice data coming from the VoIP phone is tagged with the exchanged VLAN ID; thus, regular data arriving on the switch is assigned the default PVID of the port, and the voice traffic is received on a predefined VLAN. The two types of traffic are segregated so that better service can be provided to the voice traffic.

Note: The IP phone must support LLDP-MED to accept the VLAN ID and CoS information from the switch.

voice vlan (Global Config)

M4250

M4350

Use this command to enable the Voice VLAN capability on the switch.

Default	Disabled
Format	<code>voice vlan</code>
Mode	Global Config

no voice vlan (Global Config)

Use this command to disable the Voice VLAN capability on the switch.

Format	<code>no voice vlan</code>
Mode	Global Config

voice vlan (Interface Config)

M4250**M4350**

Use this command to enable the Voice VLAN capability on the interface or range of interfaces.

Default	Disabled
Format	<code>voice vlan {vlan-id dot1p priority none untagged}</code>
Mode	Interface Config

You can configure Voice VLAN in one of four different ways.

Parameter	Description
vlan-id	Configure the IP phone to forward all voice traffic through the specified VLAN. Valid VLAN ID's are from 1 to 4093 (the max supported by the platform).
dot1p	Configure the IP phone to use 802.1p priority tagging for voice traffic and to use the default native VLAN (VLAN 0) to carry all traffic. Valid priority range is 0 to 7.
none	Allow the IP phone to use its own configuration to send untagged voice traffic.
untagged	Configure the phone to send untagged voice traffic.

no voice vlan (Interface Config)

Use this command to disable the Voice VLAN capability on the interface.

Format	<code>no voice vlan</code>
Mode	Interface Config

voice vlan auth

M4250**M4350**

This command lets the switch accept or reject voice traffic when the port is in an unauthorized state. By default, the switch rejects voice traffic when the port is in an unauthorized state.

Default	disable
Format	<code>voice vlan auth {disable enable}</code>
Mode	Interface Config

voice vlan data priority

M4250

M4350

Use this command to either trust or untrust the data traffic arriving on the Voice VLAN interface or range of interfaces being configured.

Default	trust
Format	voice vlan data priority {untrust trust}
Mode	Interface Config

voice vlan dscp

M4250

M4350

Use this command to configure the DSCP value for voice traffic on the Voice VLAN port. The value can be from 0 to 64.

Default	0
Format	voice vlan dscp value
Mode	Interface Config

no voice vlan dscp

Use this command to reset the DSCP value for voice traffic to the default value.

Format	no voice vlan dscp
Mode	Interface Config

show voice vlan

Use this command to display information about the voice VLAN. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show voice vlan [interface {unit/slot/port all}]
Mode	Privileged EXEC

If you do not specify an interface, only the global mode of the Voice VLAN is displayed.

Term	Definition
Administrative Mode	The Global Voice VLAN mode.

If you do specify an interface, more information is displayed.

Term	Definition
Interface	The Voice VLAN interface ID.
Voice VLAN Interface Mode	The admin mode of the Voice VLAN on the port.
Voice VLAN CoS Override	The CoS override option for the voice traffic arriving on the port.
Voice VLAN DSCP Value	The DSCP value for the Voice VLAN on the port.
Voice VLAN Port Status	The port status for the Voice VLAN.
Voice VLAN Authentication	The authentication state of the Voice VLAN on the port.
Voice VLAN Operational Value	The operational value of the Voice VLAN on the port.

Precision Time Protocol Commands

Note: Precision Time Protocol (PTP)-transparent clocks (TC) and audio-video bridging (AVB) are mutually exclusive. You can either globally specify the settings for PTP-TC, as described in this section, or for 802.1AS and MRP, both of which configure the switch for AVB (see [Audio Video Bridging Commands on page 873](#)).

Note: For M4350 series SMPTE-capable switches, you can configure both PTP-BC and PTP-TC on different ports of the same switch, as long as each PTP type is on a separate VLAN. For a list of M4350 series SMPTE-capable switches, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This section describes the commands you can use to configure Precision Time Protocol (PTP), including the end-to-end (E2E) transparent clock feature that is supported on all M4250 and M4350 series switch models, and the boundary clock/grandmaster clock feature that is supported on M4350 series SMPTE-capable switches (see [NETGEAR AV and IT Managed Switches M4350 Series](#)).

ptp clock e2e-transparent

M4250**M4350**

This command enables the PTP E2E transparent clock at system level (that is, globally) or for an interface.

Default	Enabled at system level and for all interfaces
Format	<code>ptp clock e2e-transparent</code>
Mode	Global Config Interface Config

In Global Config mode, the command applies the PTP transparent clock configuration to all physical ports and LAGs on the switch. In Interface Config mode, the command provides a next-level control so you can disable this feature selectively for an individual physical port or LAG.

You can configure the PTP transparent clock for physical ports and LAGs, but not for a VLAN. When you configure the PTP transparent clock on a LAG, the configuration is applied to all member ports.

no ptp clock e2e-transparent

This command disables the PTP E2E transparent clock at system level or for an interface.

Format	<code>no ptp clock e2e-transparent</code>
Mode	Global Config Interface Config

ptp clock-operation

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command enables PTP one-step boundary clock operation. The default setting is two-step mode. The modes function as follows:

- One-step clock mode: The clock timestamps the sync message as it exits the switch but no follow-up message is sent.

- Two-step clock mode: The clock timestamps the sync message as it exits the switch and then sends a follow-up message that includes the egress timestamp of the sync message.

Default	two-step
Format	<code>ptp clock-operation one-step</code>
Mode	Global Config

`no ptp clock-operation one-step`

This command resets the PTP clock operation to the default mode, which is two-step operation.

Format	<code>no ptp clock-operation one-step</code>
Mode	Global Config

`ptp source`

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the PTP source IPv4 or IPv6 IP address, which is the IP address that is used for the multicast transport mode. This command does not apply to L2 transport mode.

Default	None
Format	<code>ptp source {ipv4-address <i>ipaddr</i> ipv6-address <i>ip6addr</i>}</code>
Mode	Global Config

`no ptp source`

This command removes the configured IPv4 or IPv6 PTP source address. The source address is reset to the IP address of the L3 interface on which the packets are transmitted.

Format	<code>no ptp source {ipv4-address ipv6-address}</code>
Mode	Global Config

ptp priority1

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the local clock priority 1 value, which determines which switch that is capable of functioning as a grandmaster clock is elected to be the active grandmaster clock in the network. A lower value takes precedence over a higher value.

Default	128
Format	ptp priority1 {0-255}
Mode	Global Config

no ptp priority1

This command resets the local clock priority 1 to the default, which is 128.

Format	no ptp priority1
Mode	Global Config

ptp priority2

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the local clock priority 2 value. If the priority 1 value of two switches that are capable of functioning as a grandmaster clock is identical, the priority 2 value determines which switch is elected to be the active grandmaster clock in the network. A lower value takes precedence over a higher value.

Default	128
Format	ptp priority2 {0-255}
Mode	Global Config

no ptp priority2

This command resets the local clock priority 1 to the default, which is 128.

Format	no ptp priority2
Mode	Global Config

ptp profile aes-r16-2016

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command enables a clock profile that inter-operates between SMPTE and AES67 clock profiles.

Default	None
Format	ptp profile aes-r16-2016
Mode	Global Config

no ptp profile

This command resets the aes-r16-2016 profile to the default profile.

Format	no ptp profile
Mode	Global Config

ptp profile aes-r16-2016 announce

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the announce interval, which is the period between successive Announce messages in logarithm to base 2 format. This command is specific to the specified PTPv2 profile.

Default	0
Format	<code>ptp profile aes-r16-2016 announce {0 1}</code>
Mode	Global Config

`no ptp profile aes-r16-2016 announce`

This command resets the announce interval to the default value of 0. This command is specific to the specified PTPv2 profile.

Format	<code>no ptp aes-r16-2016 announce</code>
Mode	Global Config

`ptp profile aes-r16-2016 delay-request`

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the delay request, which is the period between successive Delay-Request messages from the boundary clock to the grandmaster clock, in logarithm to base 2 format. Delay-Request messages help to calculate the path delay and support a value from -4 to 5. This command is specific to the specified PTPv2 profile.

Default	-3
Format	<code>ptp profile aes-r16-2016 delay-request {-4-5}</code>
Mode	Global Config

`no ptp profile aes-r16-2016 delay-request`

This command resets the delay request interval to the default value of -3. This command is specific to the specified PTPv2 profile.

Format	<code>no ptp aes-r16-2016 delay-request</code>
Mode	Global Config

ptp profile aes-r16-2016 domain

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the PTP domain identifier, which represent one of more ordinary or boundary clocks that communicate with each other, and a single grandmaster clock. Although more than one switch can be capable of functioning as a grandmaster in the network, only one switch can the active grandmaster clock. This command is specific to the specified PTPv2 profile.

Default	0
Format	ptp profile aes-r16-2016 domain {0-127}
Mode	Global Config

no ptp profile aes-r16-2016 domain

This command resets the PTP domain identifier to the default value of 0. This command is specific to the specified PTPv2 profile.

Format	no ptp aes-r16-2016 domain
Mode	Global Config

ptp profile aes-r16-2016 sync

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the sync interval with a value from -4 to 1. The sync interval is the period between successive Sync messages, in logarithm to base 2 format. This command is specific to the specified PTPv2 profile.

Default	-3

Format	<code>ptp profile aes-r16-2016 sync {-4-1}</code>

Mode	Global Config

`no ptp profile aes-r16-2016 sync`

This command resets the sync interval to the default value of –3. This command is specific to the specified PTPv2 profile.

Format	<code>no ptp aes-r16-2016 sync</code>

Mode	Global Config

`ptp profile aes67`

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command enables the AES67 profile, which is a clock profile for connecting audio devices over a common PTP profile.

Default	None

Format	<code>ptp profile aes67</code>

Mode	Global Config

`no ptp profile`

This command resets the aes67 profile to the default profile.

Format	<code>no ptp profile</code>

Mode	Global Config

ptp profile aes67 announce

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the announce interval to a value from 0 to 4. The announce interval is the period between successive Announce messages in logarithm to base 2 format. This command also sets the time-out count to a value from 2 to 10. The time-out count is the number of Announce messages that are not acknowledged before the switch determines that the grandmaster clock is not transmitting. This command is specific to the specified PTPv2 profile.

Default	Interval: 1 Time-out count: 3
Format	ptp profile aes67 announce {0-4} [timeout-count {2-10}]
Mode	Global Config

no ptp profile aes67 announce

This command resets the announce interval to the default value of 1. This command is specific to the specified PTPv2 profile. If you add the optional **timeout-count** keyword, the command resets the time-out count to the default value of 3.

Format	no ptp aes67 announce [timeout-count]
Mode	Global Config

ptp profile aes67 delay-request

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the delay request to a value from -3 to 5. The delay request is the period between successive Delay-Request messages from the boundary clock to the grandmaster

clock, in logarithm to base 2 format. Delay-Request messages help to calculate the path delay. This command is specific to the specified PTPv2 profile.

Default	0
Format	<code>ptp profile aes67 delay-request {-3-5}</code>
Mode	Global Config

`no ptp profile aes67 delay-request`

This command resets the delay request interval to the default value of 0. This command is specific to the specified PTPv2 profile.

Format	<code>no ptp aes67 delay-request</code>
Mode	Global Config

`ptp profile aes67 domain`

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the PTP domain identifier, which represent one of more ordinary or boundary clocks that communicate with each other, and a single grandmaster clock. Although more than one switch can be capable of functioning as a grandmaster in the network, only one switch can the active grandmaster clock. This command is specific to the specified PTPv2 profile.

Default	0
Format	<code>ptp profile aes67 domain {0-127}</code>
Mode	Global Config

`no ptp profile aes67 domain`

This command resets the PTP domain identifier to the default value of 0. This command is specific to the specified PTPv2 profile.

Format	<code>no ptp aes67 domain</code>
Mode	Global Config

ptp profile aes67 sync

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the sync interval to a value from -4 to 1. The sync interval is the period between successive Sync messages, in logarithm to base 2 format. This command is specific to the specified PTPv2 profile.

Default	-3
Format	ptp profile aes67 sync {-4-1}
Mode	Global Config

no ptp profile aes67 sync

This command resets the sync interval to the default value of -3. This command is specific to the specified PTPv2 profile.

Format	no ptp aes67 sync
Mode	Global Config

ptp profile default

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command enables the default PTPv2 profile.

Default	None
Format	ptp profile default
Mode	Global Config

ptp profile default announce

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the announce interval to a value from 0 to 4. The announce interval is the period between successive Announce messages in logarithm to base 2 format. This command also sets the time-out count to a value from 2 to 10. The time-out count is the number of Announce messages that are not acknowledged before the switch determines that the grandmaster clock is not transmitting. This command is specific to the specified PTPv2 profile.

Default	Interval: 1 Time-out count: 3
Format	<code>ptp profile default announce {0-4} [timeout-count {2-10}]</code>
Mode	Global Config

no ptp profile default announce

This command resets the announce interval to the default value of 1. If you add the optional **timeout-count** keyword, the command resets the time-out count to the default value of 3. This command is specific to the specified PTPv2 profile.

Format	<code>no ptp default announce [timeout count]</code>
Mode	Global Config

ptp profile default delay-request

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the delay request to a value from 0 to 5. The delay request is the period between successive Delay-Request messages from the boundary clock to the grandmaster clock, in logarithm to base 2 format. Delay-Request messages help to calculate the path delay. This command is specific to the specified PTPv2 profile.

Default	0
Format	<code>ptp profile default delay-request {0-5}</code>
Mode	Global Config

`no ptp profile default delay-request`

This command resets the delay request interval to the default value of 0. This command is specific to the specified PTPv2 profile.

Format	<code>no ptp default delay-request</code>
Mode	Global Config

`ptp profile default domain`

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the PTP domain identifier, which represent one of more ordinary or boundary clocks that communicate with each other, and a single grandmaster clock. Although more than one switch can be capable of functioning as a grandmaster in the network, only one switch can be the active grandmaster clock. This command is specific to the specified PTPv2 profile.

Default	0
Format	<code>ptp profile default domain {0-127}</code>
Mode	Global Config

`no ptp profile default domain`

This command resets the PTP domain identifier to the default value of 0. This command is specific to the specified PTPv2 profile.

Format	<code>no ptp default domain</code>
Mode	Global Config

ptp profile default sync

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the sync interval to a value from -1 to 1. The sync interval is the period between successive Sync messages, in logarithm to base 2 format. This command is specific to the specified PTPv2 profile.

Default	0
Format	ptp profile default sync {-1-1}
Mode	Global Config

no ptp profile default sync

This command resets the sync interval to the default value of 0. This command is specific to the specified PTPv2 profile.

Format	no ptp default sync
Mode	Global Config

ptp profile default transport

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the transport and transmission protocol. This command is specific to the specified PTPv2 profile.

Default	Ethernet
Format	ptp profile default transport {ethernet ipv4 ipv6}
Mode	Global Config

no ptp profile default transport

This command resets the transport and transmission protocol to the default, which is Ethernet. This command is specific to the specified PTPv2 profile.

Format	no ptp default transport

Mode	Global Config

ptp profile smpte-2059-2

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command enables a clock profile for video traffic.

Default	None

Format	ptp profile smpte-2059-2

Mode	Global Config

no ptp profile

This command resets the smpte-2059-2 profile to the default profile.

Format	no ptp profile

Mode	Global Config

ptp profile smpte-2059-2 announce

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the announce interval to a value from -3 to 1. The announce interval is the period between successive Announce messages in logarithm to base 2 format. This command also sets the time-out count to a value from 2 to 10. The time-out value is the

number of Announce messages that are not acknowledged before the switch determines that the grandmaster clock is not transmitting. This command is specific to the specified PTPv2 profile.

Default	Interval: 0 Time-out count: 3
Format	<code>ptp profile smpte-2059-2 announce {-3-1} [timeout-count {2-10}]</code>
Mode	Global Config

`no ptp profile smpte-2059-2 announce`

This command resets the announce interval to the default value of 0 and the time-out count to 3. If you add the optional **timeout-count** keyword, the command resets the time-out count to the default value of 3. This command is specific to the specified PTPv2 profile.

Format	<code>no ptp smpte-2059-2 announce [timeout-count]</code>
Mode	Global Config

`ptp profile smpte-2059-2 delay-request`

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the delay request to a value from -7 to 4. The delay request is the period between successive Delay-Request messages from the boundary clock to the grandmaster clock, in logarithm to base 2 format. Delay-Request messages help to calculate the path delay. This command is specific to the specified PTPv2 profile.

Default	-3
Format	<code>ptp profile smpte-2059-2 delay-request {-7-4}</code>
Mode	Global Config

no ptp profile smpte-2059-2 delay-request

This command resets the delay request interval to the default value of –3. This command is specific to the specified PTPv2 profile.

Format	no ptp smpte-2059-2 delay-request

Mode	Global Config

ptp profile smpte-2059-2 domain

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the PTP domain identifier, which represent one of more ordinary or boundary clocks that communicate with each other, and a single grandmaster clock. Although more than one switch can be capable of functioning as a grandmaster in the network, only one switch can be the active grandmaster clock. This command is specific to the specified PTPv2 profile.

Default	0

Format	ptp profile smpte-2059-2 domain {0-127}

Mode	Global Config

no ptp profile smpte-2059-2 domain

This command resets the PTP domain identifier to the default value of 0. This command is specific to the specified PTPv2 profile.

Format	no ptp smpte-2059-2 domain

Mode	Global Config

ptp profile smpte-2059-2 sync

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the sync interval to a value from -7 to -1 . The sync interval is the period between successive Sync messages, in logarithm to base 2 format. This command is specific to the specified PTPv2 profile.

Default	-3
Format	<code>ptp profile smpte-2059-2 sync {-7--1}</code>
Mode	Global Config

no ptp profile smpte-2059-2 sync

This command resets the sync interval to the default value of -3 . This command is specific to the specified PTPv2 profile.

Format	<code>no ptp smpte-2059-2 sync</code>
Mode	Global Config

ptp profile smpte-2059-2 transport

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the transport and transmission protocol. This command is specific to the specified PTPv2 profile.

Default	IPv4
Format	<code>ptp profile smpte-2059-2 transport {ipv4 ipv6}</code>
Mode	Global Config

no ptp profile smpte-2059-2 transport

This command resets the transport and transmission protocol to the default, which is IPv4. This command is specific to the specified PTPv2 profile.

Format	no ptp smpte-2059-2 transport

Mode	Global Config

ptp path-trace

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command includes path-trace TLVs in Announce messages.

Format	ptp path-trace

Mode	Global Config

no ptp path-trace

This command excludes path-trace TLVs from Announce messages.

Format	no ptp path-trace

Mode	Global Config

ptp logging

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command enables logging of PTP traffic at the specified severity level from 0 to 7. The log severity levels are 0 (emergency), 1 (alert), 2 (critical), 3, (error), 4 (warning), 5 (notice), 6 (info), and 7 (debug).

Default	5 (notice)
Format	<code>ptp logging {0-7}</code>
Mode	Global Config Interface Config

no ptp logging

This command resets the PTP logging level to the default, which is 5 (notice).

Format	<code>no ptp logging</code>
Mode	Global Config Interface Config

ptp ieee version 2.0

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command sets the PTP operating version to 2.0 for M4350 series SMPTE-capable switches.

Default	2.1
Format	<code>ptp ieee version 2.0</code>
Mode	Global Config

no ptp ieee version 2.0

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

This command reverts the PTP operating version to the default version 2.1.

Format	no ptp ieee version 2.0

Mode	Global Config

show ptp clock e2e-transparent

M4250

M4350

Use this command to display the operational and configuration status of the PTP E2E transparent clock, both at system level and at interface level.

Format	show ptp clock e2e-transparent

Mode	Privileged Exec Global Config

Term	Definition
Interface	The interface on which the feature is configured.
Configured Mode	The configuration status of the PTP E2E transparent clock on the interface
Operational Mode	The operational status of the PTP E2E transparent clock on the interface.

Command example:

```
(NETGEAR Switch) #show ptp clock e2e-transparent
```

```
PTP TC mode..... Enabled
```

Interface	Configured Mode	Operational Mode
-----	-----	-----
1/1/1	Enabled	Disabled
1/1/2	Enabled	Disabled
1/1/3	Enabled	Disabled
1/1/4	Enabled	Disabled
1/1/5	Enabled	Disabled
1/1/6	Enabled	Disabled
1/1/7	Enabled	Disabled
1/1/8	Enabled	Disabled

show ptp interface

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

Use this command to display the status of the PTP interface.

Format	show ptp interface {unit/slot/port summary}
Mode	Privileged Exec Global Config
Parameter	Description
unit/slot/port	The <i>unit/slot/port</i> keyword specifies the interface.
summary	The <i>summary</i> keyword specifies a summary of information for the switch,
Term	Definition
Interface fields	
PTP Interface Admin Mode	The administrative mode of the interface.
PTP Interface Oper Mode	The operational mode of the interface.
Port state	The port state can be timeTransmitter (grandmaster clock), timeReceiver (secondary clock), Passive, Uncalibrated, Faulty, or NA.
PTP capable	Indicates if the port is up and configured with an IP address.
Summary fields	
Configured Mode	The administrative mode of the interface.
State	The port state can be timeTransmitter (grandmaster clock), timeReceiver (secondary clock), Passive, Uncalibrated, Faulty, or NA.
Operational Mode	The operational mode of the interface.

Command example:

```
(Switch) (Config)#show ptp interface 1/0/2
```

```
PTP Interface Admin Mode.....Disabled
PTP Interface Oper Mode.....Disabled
Port state.....FAULTY
```

PTP capable.....No

Command example:

```
(Switch) (Config)#show ptp interface summary
```

Interface	Configured Mode	State	Operational Mode
-----	-----	-----	-----
1/0/1	Disabled	NA	Disabled
1/0/2	Disabled	NA	Disabled
1/0/3	Disabled	NA	Disabled
1/0/4	Disabled	NA	Disabled
1/0/5	Disabled	NA	Disabled
1/0/6	Disabled	NA	Disabled
1/0/7	Disabled	NA	Disabled
1/0/8	Disabled	NA	Disabled
1/0/9	Disabled	NA	Disabled
1/0/10	Disabled	NA	Disabled
1/0/11	Disabled	NA	Disabled
1/0/12	Disabled	NA	Disabled
1/0/13	Disabled	NA	Disabled
1/0/14	Disabled	NA	Disabled
1/0/15	Disabled	NA	Disabled
1/0/16	Disabled	NA	Disabled
1/0/17	Disabled	NA	Disabled
1/0/18	Disabled	NA	Disabled
1/0/19	Disabled	NA	Disabled

show ptp boundary-clock

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

Use this command to display the local clock information.

Format	show ptp boundary-clock
Mode	Privileged Exec Global Config

Term	Definition
PTP device type	The clock type.
PTP device profile	The configured PTP profile.
PTP clock role type	Time transmitter clock or time receiver clock.
Clock operation mode	One-step mode or two-step mode.
Parent Clock operation mode	One-step mode or two-step mode of the parent clock. For devices that do not respond to PTP management messages, the output displays <i>Not available</i> . For master devices, the output displays <i>Not applicable</i> .
Clock domain	The domain to which the PTP instances belong.
Number of PTP ports	The number of ports that are available for PTP operation.
Clock class	The local clock class.
Clock accuracy	The accuracy of the local clock.
Offset	The offset scaled log variance of the grandmaster clock.
Steps removed	The number of hops that the grandmaster clock is removed from the PTP clock.
Mean path delay	The calculated delay for end-to-end delay measurement. This is not applicable to a peer-to-peer configuration.

Command example:

```
(Switch) (Config)#show ptp boundary-clock
```

```
PTP device type..... Boundary clock
PTP device profile..... Default
PTP clock role type..... Master
Clock operation mode..... two-step
Parent Clock operation mode..... Not applicable
Clock domain..... 0
Number of PTP ports..... 44
Clock class..... 248
Clock accuracy..... 0x23
Offset..... 0.0
Steps removed..... 0
Mean path delay..... 0.0
```

show ptp parent

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

Use this command to display the configuration of the parent clock to which the local clock is synchronized in boundary clock mode.

Format	show ptp parent
Mode	Privileged Exec Global Config
Term	Definition
Parent clock	
Clock identity	The identify of the parent clock.
Offset	The offset scaled log variance of the parent clock.
Clock phase change rate	The phase change rate of the parent clock.
Grandmaster clock	
Clock identity	The identity of the grandmaster clock.
Clock class	The class of the grandmaster clock.
Clock accuracy	The accuracy of the grandmaster clock.
Offset	The offset scaled log variance of the grandmaster clock.
Priority1	The priority 1 value of the grandmaster clock.
Priority2	The priority 2 value of the grandmaster clock.

Command example:

```
(Switch) (Config)#show ptp parent
```

```
(M4350-16V4C) (Config)#show ptp parent
```

```
Parent clock:
Clock identity..... e046ee.ffff.36a77f
Offset..... 0xffff
Clock phase change rate..... 0x7fffffff
Grandmaster clock:
```



```

Clock identity..... e046ee.ffff.36a77f
Clock class..... 248
Clock accuracy..... 0x23
Offset..... 0xffff
Priority1..... 128
Priority2..... 128

```

show ptp path-trace

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

Use this command to display the list of clocks, starting with the grandmaster clock up to, but not including, the current boundary clock.

Format	show ptp path-trace
Mode	Privileged Exec Global Config
Term	Definition
Clock Identity	The clock identifier.

Command example:

```
(Switch) (Config) #show ptp path-trace
```

```

Clock Identity
-----
001102.ffff.000002

```

show ptp statistics

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

Use this command to display the PTP interface statistics.

Format	<code>show ptp statistics unit/slot/port</code>
Mode	Privileged Exec Global Config
Parameter	Description
unit/slot/port	The <i>unit/slot/port</i> keyword specifies the interface.

Command example:

```
(Switch) (Config)#show ptp statistics 1/0/5
```

```
Announce messages transmitted..... 1
Announce messages received..... 40
Announce receipt timeouts..... 0
Sync messages transmitted..... 0
Sync messages received..... 20
Sync messages mismatched..... 0
Sync receipt timeouts..... 0
Followup messages transmitted..... 0
Followup messages received..... 0
Followup messages mismatched..... 0
Delay_Req messages transmitted..... 15
Delay_Req messages received..... 0
Pdelay_Req messages transmitted..... 0
Pdelay_Req messages received..... 0
Pdelay_Resp messages transmitted..... 0
Pdelay_Resp messages received..... 0
Delay_Resp messages transmitted..... 0
Delay_Resp messages received..... 15
Pdelay_Resp_Followup messages transmitted..... 0
Pdelay_Resp_Followup messages received..... 0
Signaling messages transmitted..... 1
Signaling messages received..... 0
Management messages transmitted..... 0
Management messages received..... 0
```

show ptp summary

M4350

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

Use this command to display the settings of the local clock and the active PTP profile.

Format	show ptp summary
Mode	Privileged Exec Global Config
Term	Definition
PTP global admin mode	The configured PTP admin mode.
PTP process running	Indicates if the PTP process is running.
Grandmaster capable	Indicates if the device is capable of becoming a grandmaster clock.
Local clock priority1	The priority 1 value of the PTP local clock.
Local clock priority2	The priority 2 value of the PTP local clock.
Domain identifier	The domain identifier, which represents the logical grouping of all PTP instances to a particular grandmaster clock or domain.
Announce interval	The configured mean time interval between successive Announce messages in logarithm to base 2 format.
Announce receipt timeout	The number of Announce intervals that must pass without receipt of an Announce PDU before the grandmaster clock is considered to be no longer transmitting.
Sync interval	The configured mean time interval between successive Sync messages in logarithm to base 2 format.
Delay-request interval	The configured mean time interval between successive Delay_Req messages in logarithm to base 2 format. This information is useful if the delay measurement mechanism is end-to-end.
Transport	The transport protocol that is used on the communication path (IPv4, IPv6, or Ethernet).
Communication model	The message type that is used for PTP communication (unicast, multicast, or hybrid, which combines unicast and multicast).
Delay measurement mechanism	The delay mechanism: end-to-end (e2e) or peer-to-peer (p2p). The default is e2e.

Term	Definition
Source IPv4 address	The configured source IPv4 address.
Source IPv6 address	The configured source IPv6 address.
PTP Logging Level	The configured logging level for PTP log messages.
Local clock identity	The identity of the local clock.

Command example:

```
(Switch) (Config) #show ptp summary
```

```
PTP global admin mode..... Disabled
PTP process running?..... Yes
Grandmaster capable..... Yes
Local clock priority1..... 128
Local clock priority2..... 128
Domain identifier..... 0
Announce interval..... 1
Announce timeout..... 3
Sync interval..... 0
Delay-request interval..... 0
Transport..... L2
Communication model..... Multicast
Delay measurement mechanism..... e2e
Source IPv4 address..... NA
Source IPv6 address..... NA
PTP Logging Level..... 5
Local clock identity..... e046ee.ffff.36a77f
```

show ptp time-properties**M4350**

Note: This command applies only to M4350 series SMPTE-capable switches, which can support boundary clock operation. For a list of these models, see [NETGEAR AV and IT Managed Switches M4350 Series](#).

Use this command to display the PTP clock time attributes.

Format	show ptp time-properties
Mode	Privileged Exec Global Config

Term	Definition
Current UTC offset	The UTC offset value.
Leap61	A Boolean value: 1 indicates that the last minute of the day contains 61 seconds; 0 indicates that the time scale is not PTP.
Leap59	A Boolean value: 1 indicates that the last minute of the day contains 59 seconds; 0 indicates that the time scale is not PTP.
Current UTC offset valid	A Boolean value: 1 indicates that the UTC offset value, Leap61 value, and Leap59 value are known to be correct; 0 indicates otherwise.
PTP timescale	A Boolean value: 1 indicates that the time scale of the GM is PTP; 0 indicates that the time scale is not PTP.
Time traceable	A Boolean value: 1 indicates that the time scale is traceable to a primary reference; 0 indicates that the times scale is not traceable.
Frequency traceable	A Boolean value: 1 indicates that the frequency determining the time scale is traceable to a primary reference; 0 indicates that the times scale is not traceable.
Time source	The source of the time that is used the GM PTP instance.

Command example:

```
(NETGEAR Switch) (Config) #show ptp time-properties
```

```
Current UTC offset..... 37
Leap61..... 0
Leap59..... 0
Current UTC offset valid..... 0
PTP timescale..... 1
Time traceable..... 0
Frequency traceable..... 0
Time source..... 0xa0
```

Provisioning (IEEE 802.1p) Commands

This section describes the commands you use to configure provisioning (IEEE 802.1p,) which allows you to prioritize ports.

vlan port priority all

M4250

M4350

This command configures the port priority assigned for untagged packets for all ports presently plugged into the device. The range for the priority is 0-7. Any subsequent per port configuration will override this configuration setting.

Format	vlan port priority all <i>priority</i>
Mode	Global Config

vlan priority

M4250

M4350

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface. The range for the priority is 0–7.

Default	0
Format	vlan priority <i>priority</i>
Mode	Interface Config

Asymmetric Flow Control Commands

When in asymmetric flow control mode, the switch responds to PAUSE frames received from a peer by stopping packet transmission, but the switch does not initiate MAC control PAUSE frames.

When you configure the switch in asymmetric flow control (or no flow control mode), the device is placed in egress drop mode. Egress drop mode maximizes the throughput of the system at the expense of packet loss in a heavily congested system, and this mode avoids head-of-line blocking.

flowcontrol

M4250

M4350

Use this command to enable the symmetric or asymmetric flow control on the switch. Asymmetric flow control means you can enable Rx Pause only but not Tx Pause.

Default	Flow control is disabled.
Format	<code>flowcontrol {symmetric asymmetric}</code>
Mode	Interface Config

no flowcontrol

This command disables flow control.

Format	<code>no flowcontrol</code>
Mode	Global Config

show flowcontrol

M4250

M4350

Use this command to display the IEEE 802.3 Annex 31B flow control settings and status for a specific interface or all interfaces. The command also displays 802.3 Tx and Rx pause counts. Priority Flow Control frames counts are not displayed. If the port is enabled for priority flow control, operational flow control status is displayed as Inactive. Operational flow control status for stacking ports is always displayed as N/A. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show flowcontrol [interface <i>unit/slot/port</i>]</code>
Mode	Privileged Exec

Command example:

```
(NETGEAR Switch) #show flowcontrol
```

```
Admin Flow Control: Symmetric
```

Port	Flow Control Oper	RxPause	TxPause
-----	-----	-----	-----
0/1	Active	310	611
0/2	Inactive	0	0

Command example:

```
(NETGEAR Switch) #show flowcontrol interface 0/1
```

```
Admin Flow Control: Symmetric
```

Port	Flow Control Oper	RxPause	TxPause
-----	-----	-----	-----
0/1	Active	310	611

Protected Port Commands

This section describes commands you use to configure and view protected ports on a switch. Protected ports do not forward traffic to each other, even if they are on the same VLAN. However, protected ports can forward traffic to all unprotected ports in their group. Unprotected ports can forward traffic to both protected and unprotected ports. Ports are unprotected by default.

If an interface is configured as a protected port, and you add that interface to a Port Channel or Link Aggregation Group (LAG), the protected port status becomes operationally disabled on the interface, and the interface follows the configuration of the LAG port. However, the protected port configuration for the interface remains unchanged. Once the interface is no longer a member of a LAG, the current configuration for that interface automatically becomes effective.

switchport protected (Global Config)

M4250**M4350**

Use this command to create a protected port group. The *groupid* parameter identifies the set of protected ports. Use the *name* parameter to assign a name to the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.

Note: Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default	unprotected
Format	switchport protected <i>groupid</i> [<i>name name</i>]
Mode	Global Config

no switchport protected (Global Config)

Use this command to remove a protected port group. The *groupid* parameter identifies the set of protected ports. The *name* parameter specifies the name to remove from the group.

Format	no switchport protected <i>groupid</i>
Mode	Global Config

switchport protected (Interface Config)

M4250**M4350**

Use this command to add an interface to a protected port group. The *groupid* parameter identifies the set of protected ports to which this interface is assigned. You can only configure an interface as protected in one group.

Note: Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default	unprotected
Format	<code>switchport protected <i>groupid</i></code>
Mode	Interface Config

no switchport protected (Interface Config)

Use this command to configure a port as unprotected. The *groupid* parameter identifies the set of protected ports to which this interface is assigned.

Format	<code>no switchport protected <i>groupid</i></code>
Mode	Interface Config

show switchport protected

M4250

M4350

This command displays the status of all the interfaces, including protected and unprotected interfaces.

Format	<code>show switchport protected <i>groupid</i></code>
Mode	Privileged EXEC User EXEC

Term	Definition
Group ID	The number that identifies the protected port group.
Name	An optional name of the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.
List of Physical Ports	List of ports, which are configured as protected for the group identified with <i>groupid</i> . If no port is configured as protected for this group, this field is blank.

show interfaces switchport (for a group ID)

M4250

M4350

This command displays the status of the interface (protected or unprotected) under the *groupid*. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show interfaces switchport unit/slot/port groupid</code>
Mode	Privileged EXEC User EXEC
Term	Definition
Name	A string associated with this group as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. This field is optional.
Protected	Indicates whether the interface is protected or not. It shows TRUE or FALSE. If the group is a multiple groups then it shows TRUE in Group <i>groupid</i> .

Private Group Commands

This section describes commands that are used to configure a private group and view the configuration information of a private group.

You can use a private group to create a group of ports that either can or cannot share traffic with each other in the same VLAN group. The main purpose of a private group is to isolate a group of users from another group of users without using a VLAN.

`switchport private-group`

M4250

M4350

This command assigns one port or a range of ports to a private group. You specify the private group by either its name or its identifier.

The ingress traffic from a port in a private group can be forwarded to other ports either in the same private group or outside the private group but in the same VLAN.

By default, a port does not belong to any private group. A port cannot be in more than one private group. To change the membership of a port in a private group, first remove the port from the private group.

Format	<code>switchport private-group [privategroup-name privategroup-id]</code>
Mode	Interface Config

`no switchport private-group`

This command removes a port from to a private group.

Format	<code>no switchport private-group [privategroup-name privategroup-id]</code>
Mode	Interface Config

private-group name

M4250

M4350

This command creates a private group with a name or an identifier. The name string can be up to 24 bytes of non-blank characters. A total number of 192 of private groups is supported. Therefore, the group identifier can be from 1 to 192.

The *private-group-id* parameter is optional. If you do not specify a group identifier, the identifier is assigned automatically.

The optional mode for the group can be either isolated or community. If the private group is 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 for the private group is community mode, allowing each member port to forward traffic to other members in the same group, but not to members in other groups.

Format	<code>private-group name <i>privategroup-name</i> [<i>private-group-id</i>] [mode {community isolated}]</code>
Mode	Global Config

no private-group name

This command removes a private group.

Format	<code>no private-group name <i>privategroup-name</i></code>
Mode	Global Config

show private-group

M4250

M4350

This command displays information about a private group. If you do not specify a group name, group identifier, or port, the command displays information about all private groups. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show private-group [<i>private-group-name</i> <i>private-group-id</i> port <i>unit/slot/port</i>]</code>
Mode	Privileged EXEC

Term	Description
Interface	A valid port number.
Port VLANID	The VLAN ID that is associated with the port.
Private Group ID	The identifier of the private group (from 1 to 192).
Private Group Name	The name of the private group. The name string can be up to 24 bytes of non-blank characters.
Private Group Mode	The mode of the private group. The mode can be either isolated or community.

GARP Commands

This section describes the commands you use to configure Generic Attribute Registration Protocol (GARP) and view GARP status. The commands in this section affect both GARP VLAN Registration Protocol (GVRP) and GARP Multicast Registration Protocol (GMRP). GARP is a protocol that allows client stations to register with the switch for membership in VLANs (by using GVMP) or multicast groups (by using GVMP).

set garp timer join

M4250

M4350

This command sets the GVRP join time per GARP for one interface, a range of interfaces, or all interfaces. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or reregistering) membership for a VLAN or multicast group. This command has an effect only when GVRP is enabled. The time is from 10 to 100 centiseconds. The value 20 centiseconds is 0.2 seconds.

Default	20
Format	<code>set garp timer join centiseconds</code>
Mode	Interface Config Global Config

no set garp timer join

This command sets the GVRP join time to the default and only has an effect when GVRP is enabled.

Format	<code>no set garp timer join</code>
Mode	Interface Config Global Config

set garp timer leave

M4250**M4350**

This command sets the GVRP leave time for one interface, a range of interfaces, or all interfaces or all ports and only has an effect when GVRP is enabled. Leave time is the time to wait after receiving an deregister request for a VLAN or a multicast group before deleting the VLAN entry. This can be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. The leave time is 20 to 600 centiseconds. The value 60 centiseconds is 0.6 seconds. The leave time must be greater than or equal to three times the join time.

Default	60
Format	<code>set garp timer leave <i>centiseconds</i></code>
Mode	Interface Config Global Config

no set garp timer leave

This command sets the GVRP leave time on all ports or a single port to the default and only has an effect when GVRP is enabled.

Format	<code>no set garp timer leave</code>
Mode	Interface Config Global Config

set garp timer leaveall

M4250**M4350**

This command sets how frequently Leave All PDUs are generated. A Leave All PDU indicates that all registrations will be unregistered. Participants would need to rejoin in order to maintain registration. The value applies per port and per GARP participation. The time may range from 200 to 6000 centiseconds. The value 1000 centiseconds is 10 seconds. You can use this command on all ports (Global Config mode), or on a single port or a range of ports (Interface Config mode) and it only has an effect only when GVRP is enabled. The leave all time must be greater than the leave time.

Default	1000
Format	<code>set garp timer leaveall <i>centiseconds</i></code>
Mode	Interface Config Global Config

no set garp timer leaveall

This command sets how frequently Leave All PDUs are generated the default and only has an effect when GVRP is enabled.

Format	no set garp timer leaveall
Mode	Interface Config Global Config

show garp

M4250

M4350

This command displays GARP information.

Format	show garp
Mode	Privileged EXEC User EXEC

Term	Definition
GMRP Admin Mode	The administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.
GVRP Admin Mode	The administrative mode of GARP VLAN Registration Protocol (GVRP) for the system.

GVRP Commands

This section describes the commands you use to configure and view GARP VLAN Registration Protocol (GVRP) information. GVRP-enabled switches exchange VLAN configuration information, which allows GVRP to provide dynamic VLAN creation on trunk ports and automatic VLAN pruning.

Note: If GVRP is disabled, the system does not forward GVRP messages.

set gvrp adminmode

M4250

M4350

This command enables GVRP on the system.

Default	Disabled
Format	set gvrp adminmode
Mode	Privileged EXEC

no set gvrp adminmode

This command disables GVRP.

Format	no set gvrp adminmode
Mode	Privileged EXEC

set gvrp interfacemode

M4250

M4350

This command enables GVRP on a single port (Interface Config mode), a range of ports, or all ports (Global Config mode).

Default	Disabled
Format	set gvrp interfacemode
Mode	Interface Config Global Config

no set gvrp interfacemode

This command disables GVRP on a single port (Interface Config mode) or all ports (Global Config mode). If GVRP is disabled, Join Time, Leave Time and Leave All Time have no effect.

Format	no set gvrp interfacemode
Mode	Interface Config Global Config

show gvrp configuration

M4250

M4350

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show gvrp configuration {unit/slot/port all}</code>
Mode	Privileged EXEC User EXEC
Term	Definition
Interface	The interface.
Join Timer	The interval between the transmission of GARP PDUs registering (or reregistering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is one centisecond (0.01 seconds).
Leave Timer	The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).
LeaveAll Timer	This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).
Port GMRP Mode	The GMRP administrative mode for the port, which is enabled or disabled (default). If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

GMRP Commands

This section describes the commands you use to configure and view GARP Multicast Registration Protocol (GMRP) information. Like IGMP snooping, GMRP helps control the flooding of multicast packets. GMRP-enabled switches dynamically register and de-register group membership information with the MAC networking devices attached to the same

segment. GMRP also allows group membership information to propagate across all networking devices in the bridged LAN that support Extended Filtering Services.

Note: If GMRP is disabled, the system does not forward GMRP messages.

set gmrp adminmode

M4250

M4350

This command enables GARP Multicast Registration Protocol (GMRP) on the system.

Default	Disabled
Format	set gmrp adminmode
Mode	Privileged EXEC

no set gmrp adminmode

This command disables GARP Multicast Registration Protocol (GMRP) on the system.

Format	no set gmrp adminmode
Mode	Privileged EXEC

set gmrp interfacemode

M4250

M4350

This command enables GARP Multicast Registration Protocol on a single interface (Interface Config mode), a range of interfaces, or all interfaces (Global Config mode). If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality is disabled on that interface. GARP functionality is subsequently re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Default	Disabled
Format	set gmrp interfacemode
Mode	Interface Config Global Config

no set gmrp interfacemode

This command disables GARP Multicast Registration Protocol on a single interface or all interfaces. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality is disabled. GARP functionality is subsequently re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Format	no set gmrp interfacemode

Mode	Interface Config Global Config

show gmrp configuration

M4250

M4350

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show gmrp configuration { <i>unit/slot/port</i> all}

Mode	Privileged EXEC User EXEC

Term	Definition
Interface	The <i>unit/slot/port</i> of the interface that this row in the table describes.
Join Timer	The interval between the transmission of GARP PDUs registering (or reregistering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).
Leave Timer	The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).

Term	Definition
LeaveAll Timer	This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).
Port GMRP Mode	The GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

show mac-address-table gmrp

M4250

M4350

This command displays the GMRP entries in the Multicast Forwarding Database (MFDB) table.

Format	show mac-address-table gmrp
Mode	Privileged EXEC

Term	Definition
VLAN ID	The VLAN in which the MAC Address is learned.
MAC Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	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.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

Port-Based Network Access Control Commands

This section describes the commands you use to configure port-based network access control (IEEE 802.1X, also referred to as dot1x). Port-based network access control allows you to permit access to network services only to and devices that are authorized and authenticated.

aaa authentication dot1x default

M4250**M4350**

Use this command to configure the authentication methods for port-based access to the switch. The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure.

The possible methods are as follows:

- **ias**. Uses the internal authentication server users database for authentication.
- **none**. Uses no authentication.
- **radius**. Uses the list of all RADIUS servers for authentication.

You can configure one method at the time.

Format	aaa authentication dot1x default {ias none radius}
Mode	Global Config

Command example:

```
(NETGEAR Switch) #
(NETGEAR Switch) #configure
(NETGEAR Switch) (Config)#aaa authentication dot1x default ias
(NETGEAR Switch) (Config)#aaa authentication dot1x default radius
```

no authentication dot1x default

This command disables the authentication methods for port-based access to the switch.

Format	no authentication dot1x default
Mode	Global Config

dot1x system-auth-control

M4250**M4350**

This command enables 802.1X authentication support on the switch.

Default	Disabled
Format	dot1x system-auth-control
Mode	Global Config

no dot1x system-auth-control

This command disables 802.1X authentication support on the switch. If you configure 802.1X authentication and then disable the command, the 802.1X configuration is retained and can be changed, but is not activated.

Format	no dot1x system-auth-control
Mode	Global Config

authentication port-control all

M4250

M4350

This command enables and configures the global authentication port-control mode. The interface port-control mode takes precedence over the global port-control mode.

Default	Disabled
Format	authentication port-control all {auto force-authorized force-unauthorized}
Mode	Global Config

no authentication port-control all

This command disables the global authentication port-control mode.

Format	no authentication port-control all
Mode	Global Config

authentication port-control

M4250

M4350

This command enables and configures the authentication port-control mode for an interface. The interface port-control mode takes precedence over the global port-control mode.

Default	Disabled
Format	authentication port-control {auto force-authorized force-unauthorized}
Mode	Interface Config

no authentication port-control

This command disables the authentication port-control mode for the interface.

Format	no authentication port-control
Mode	Interface Config

authentication host-mode all

M4250

M4350

This command enables and configures the global authentication host mode. The interface host mode takes precedence over the global host mode.

Default	Disabled
Format	authentication host-mode all {multi-auth multi-domain multi-host single-host multi-domain-multi-host}
Mode	Global Config

no authentication host-mode all

This command disables the global authentication host mode.

Format	no authentication host-mode all
Mode	Global Config

authentication host-mode

M4250

M4350

This command enables and configures the authentication host mode on an interface. The interface host mode takes precedence over the global host mode.

Default	multi-host
Format	authentication host-mode {multi-auth multi-domain multi-host single-host multi-domain-multi-host}
Mode	Interface Config

no authentication host-mode

This command disables the authentication host mode on an interface and sets the authentication host mode for the interface to the default setting.

Format	no authentication host-mode
Mode	Interface Config

authentication open

M4250

M4350

This command enables open authentication on the interface.

Default	Disabled
Format	authentication open
Mode	Interface Config

no authentication open

This command disables open authentication on the interface

Format	no authentication open
Mode	Interface Config

authentication critical recovery max-reauth

M4250

M4350

This command configures the number of supplicants that can be reauthenticated per second. This configuration applies to the switch, that is, to all the supplicants on all interfaces. The function is to control the switch and network load when a large number of supplicants must be re-authenticated, for example, when reinitialization is caused by a server action. For *number*, enter the number of supplicants that can be reauthenticated per second, from 1 to 50 supplicants.

Default	10
Format	authentication critical recovery max-reauth <i>number</i>
Mode	Global Config

no authentication critical recovery max-reauth

This command removes the restriction to the number of supplicants that can be reauthenticated per second and sets the number (that applies only if the restriction is enabled) to defaults.

Format	<code>no authentication critical recovery max-reauth</code>

Mode	Interface Config

clear authentication sessions

M4250

M4350

This command clears information for all authentication manager sessions on the switch or, as an option, on a specific interface. All authenticated clients are re-initialized and forced to authenticate again. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>clear authentication sessions [unit/slot/port]</code>

Mode	Privileged EXEC

clear dot1x statistics

M4250

M4350

This command resets the 802.1X statistics for the specified port or for all ports. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>clear dot1x statistics {unit/slot/port all}</code>

Mode	Privileged EXEC

clear radius statistics

M4250

M4350

This command is used to clear all RADIUS statistics.

You can clear all statistics, the accounting server statistics, or the authentication server statistics.

Format	<code>clear radius statistics {acct all auth}</code>

Mode	Privileged EXEC

dot1x eapolflood

M4250

M4350

Use this command to enable EAPOL flood support on the switch.

Default	Disabled

Format	<code>dot1x eapolflood</code>

Mode	Global Config

no dot1x eapolflood

This command disables EAPOL flooding on the switch.

Format	<code>no dot1x eapolflood</code>

Mode	Global Config

authentication dynamic-vlan enable

M4250

M4350

Use this command to enable the switch to create VLANs dynamically when a RADIUS-assigned VLAN does not exist in the switch.

Default	Disabled

Format	<code>authentication dynamic-vlan enable</code>

Mode	Global Config

no authentication dynamic-vlan enable

Use this command to prevent the switch from creating VLANs when a RADIUS-assigned VLAN does not exist in the switch.

Format	<code>no authentication dynamic-vlan enable</code>

Mode	Global Config

authentication event no-response action authorize vlan

M4250

M4350

This command configures a VLAN as the guest VLAN on an interface (or range of interfaces). The command specifies an active VLAN as an IEEE 802.1X guest VLAN. The range for *vlan-id* is from 1 to 4093.

Default	Disabled
Format	authentication event no-response action authorize vlan <i>vlan-id</i>
Mode	Interface Config

no authentication event no-response action authorize vlan

This command disables a guest VLAN on the interface.

Default	Disabled
Format	no authentication event no-response action authorize vlan
Mode	Interface Config

dot1x max-req

M4250

M4350

This command sets the maximum number of times an interface or range of interfaces transmits EAPOL EAP Request frames (excluding Request-Identity frames) before restarting the authentication process. The *count* parameter must be in the range from 1 to 20.

Default	2
Format	dot1x max-req <i>count</i>
Mode	Interface Config

no dot1x max-req

This command resets the maximum number of authentication retries for the interface or range of interfaces to its default value.

Format	no dot1x max-req
Mode	Interface Config

dot1x max-reauth-req

M4250**M4350**

This command sets the maximum number of times an interface or range of interfaces transmits an EAPOL EAP Request/Identity frame for reauthentication before timing out the supplicant. The *count* parameter must be in the range from 1 to 20.

Default	2
Format	dot1x max-reauth-req <i>count</i>
Mode	Interface Config

no dot1x max-reauth-req

This command resets the maximum number of reauthentication retries for the interface or range of interfaces to its default value.

Format	no dot1x max-reauth-req
Mode	Interface Config

authentication max-users

M4250**M4350**

Use this command to set the maximum number of clients supported on an interface (or range of interfaces) when MAC-based 802.1X authentication is enabled on the interface. The value of *count* must be in the range from 1 to 48.

Default	48
Format	authentication max-users <i>count</i>
Mode	Interface Config

no authentication max-users

This command resets the maximum number of clients allowed on an interface to its default setting.

Format	no authentication max-users
Mode	Interface Config

authentication port-control

M4250**M4350**

This command sets the authentication mode that must be used on a specified interface (or range of interfaces.) Use the following parameters:

- **auto.** Use this parameter to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server.
- **force-authorized.** Use this parameter to specify that the authenticator PAE unconditionally sets the controlled port to authorized.
- **force-unauthorized.** Use this parameter to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized.

Default	auto
Format	authentication port-control {auto force-authorized force-unauthorized}
Mode	Interface Config

no authentication port-control

This command sets the 802.1X port control mode on a specified interface to the default setting.

Format	no authentication port-control
Mode	Interface Config

mab

M4250**M4350**

If the 802.1X mode on the interface is MAC-based, you can use this command to enable MAC Authentication Bypass (MAB) on an interface. MAB is a supplemental authentication mechanism that allows 802.1X-unaware clients, such as printers, fax machines, and some IP phones, to authenticate to the network using the client MAC address as an identifier. However, you can also use MAB to authenticate 802.1x-aware clients. This command also provides options to specify the type of authentication that must be used, which can be EAP-MD5, PAP, or CHAP. If enabled, EAP-MD5 is the default setting.

Default	Disabled
Format	mab [auth-type {pap eap-md5 chap}]
Mode	Interface Config

no mab

This command disables MAB on the interface.

Format	no mab
Mode	Interface Config

mab request format attribute 1

M4250

M4350

This command sets configuration parameters that are used to format attribute1 for MAB requests to the RADIUS server. RADIUS attribute 1 is the username, which is often the client MAC address.

Default	The group size is 2 The separator is : The case is uppercase.
Format	mab request format attribute 1 groupsize {1 2 4 12} separator {- : .} [lowercase uppercase]
Mode	Global Config

Parameter	Definition
groupsize	The number of characters included in a group. In the following example, the group size is 2: 00:10:18:99:F2:B3 In the following example, the group size is 4: 0010:1899:F2B3
separator	The character that separates the group. In the following example, the separator is - (hyphen): 00-10-18-99-F2-B3 In the following example, the separator is : (colon): 00:10:18:99:F2:B3
lowercase or uppercase	The case of any letters in the user name. In the following example, the case is lowercase: 00:10:18:99:f2:b3 In the following example, the case is uppercase: 00:10:18:99:F2:B3

no mab request format attribute 1

This command resets attribute 1 formats for MAB requests to the RADIUS server to the default values.

Format	no mab request format attribute 1

Mode	Global Config

authentication periodic

M4250

M4350

This command enables reauthentication of a supplicant on the interface (or range of interfaces.)

Default	Disabled

Format	authentication periodic

Mode	Interface Config

no authentication periodic

This command disables reauthentication of a supplicant on the interface.

Format	no authentication periodic

Mode	Interface Config

authentication timer reauthenticate

M4250

M4350

If you enabled period reauthentication with the **authentication periodic** command (see the previous command), you can use the **authentication timer reauthenticate** command.

This command configures the period after which an authenticator attempts to reauthenticate a supplicant on the interface. By default, the session time-out and session termination action that are configured on the server (such as RADIUS server) are used by authenticator. You can also configure a period in seconds. For *seconds*, enter a value from 1 to 65535.

Default	server

Format	authentication timer reauthenticate {seconds server}

Mode	Interface Config

no authentication timer reauthenticate

This command sets the session time-out and session termination action to those that are configured on the server.

Format	no authentication timer reauthenticate
Mode	Interface Config

authentication timer restart

M4250

M4350

This command configures the period after which an authenticator must restart reauthentication of a supplicant on the interface. For *seconds*, enter a value from 10 to 65535.

Default	No default
Format	authentication timer restart <i>seconds</i>
Mode	Interface Config

no authentication timer restart

This command removes the configured authentication timer restart period.

Format	no authentication timer restart
Mode	Interface Config

authentication enable

M4250

M4350

Use this command to enable the dot1x authentication support on the switch. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

Default	Disabled
Format	authentication enable
Mode	Global Config

no authentication enable

This command is used to disable the dot1x authentication support on the switch.

Format	no authentication enable

Mode	Global Config

dot1x timeout

M4250

M4350

This command sets the value, in seconds, of the timer used by the authenticator on an interface (or range of interfaces). You can set time-out settings for multiple parameters.

The value for *seconds* can be from 1 to 65535 seconds.

Default	• auth-period: 30 seconds • held-period: 60 seconds • quiet-period: 60 seconds • server-timeout: 30 seconds • start-period: 30 seconds • supp-timeout: 30 seconds • tx-period: 30 seconds

Format	dot1x timeout {{auth-period <i>seconds</i> } {held-period <i>seconds</i> } {quiet-period <i>seconds</i> } {server-timeout <i>seconds</i> } {start-period <i>seconds</i> } {supp-timeout <i>seconds</i> } {tx-period <i>seconds</i> }}

Mode	Interface Config

Parameter	Definition
auth-period	The period after which the interface times out an authenticator while waiting for a response to packets other than EAPOL-Start packets.
held-period	The period that the interface waits before it sends authentication credentials after an earlier attempt failed.
quiet-period	The period during which the interface does not attempt to acquire a supplicant.
server-timeout	The period after which the interface times out the authentication server.
start-period	The interval after which one successive EAPOL-Start frame on the interface is followed by another EAPOL-Start frame.
supp-timeout	The period after which the interface times out the supplicant.
tx-period	The period after which the interface sends an EAPOL EAP Request/Identity frame to the supplicant.

no dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator on the interface to the default values. Depending on the parameter that you enter, the corresponding default value is set.

Format	no dot1x timeout {auth-period held-period quiet-period server-timeout start-period supp-timeout tx-period}

Mode	Interface Config

authentication event fail action authorize vlan

M4250

M4350

Use this command to configure the unauthenticated VLAN associated with the specified interface (or range of interfaces). This VLAN is used when the server fails to recognize the client credentials and rejects the authentication attempt. The unauthenticated VLAN ID can be from 0 to 4093. The unauthenticated VLAN must be statically configured in the VLAN database to be operational. By default, the unauthenticated VLAN ID is 0, that is, invalid and not operational.

Default	0

Format	authentication event fail action authorize vlan <i>vlan-id</i>

Mode	Interface Config

no authentication event fail action authorize vlan

This command resets the unauthenticated VLAN that is associated with the interface to its default value.

Format	no authentication event fail action authorize vlan

Mode	Interface Config

authentication event fail retry

M4250

M4350

This command configures the number of times authentication can be reattempted by a client before an interface enter the authentication fail VLAN state. The number of maximum attempts can be from 1 to 5.

Default	3
Format	<code>authentication event fail retry <i>max-attempts</i></code>
Mode	Interface Config

no authentication event fail retry

This command set the number of times authentication can be reattempted to its default value.

Format	<code>no authentication event fail retry</code>
Mode	Interface Config

dot1x user

M4250

M4350

This command adds the specified user to the list of users with access to the specified port or all ports. The *user* argument must be a configured user. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>dot1x user <i>user</i> {<i>unit/slot/port</i> all}</code>
Mode	Global Config

no dot1x user

This command removes the user from the list of users with access to the specified port or all ports.

Format	<code>no dot1x user <i>user</i> {<i>unit/slot/port</i> all}</code>
Mode	Global Config

authentication enable

M4250

M4350

This command globally enables the authentication manager. Interface configuration takes effect only if the authentication manager is enabled with this command.

Default	Disabled
Format	authentication enable
Mode	Global Config

no authentication enable

This command disables the Authentication Manager.

Format	no authentication enable
Mode	Global Config

eapol announcements

M4250

M4350

This command configures an unsecure announcement on a specific physical interface.

Default	Disabled
Format	eapol announcements
Mode	Interface Config

no eapol announcements

This command disables an unsecure announcement on a specific physical interface.

Format	no eapol announcements
Mode	Interface Config

authentication control-direction

M4250**M4350**

This command sets the authentication control direction for the traffic flow of the interface. The direction can be both (ingress and egress, which is the default setting) or in (ingress only).

Default	both
Format	authentication control-direction {both in}
Mode	Interface Config

no authentication control-direction

This command sets the authentication control direction on an interface to the default settings.

Format	no authentication control-direction
Mode	Interface Config

authentication order

M4250**M4350**

This command sets the order of authentication methods used on a port. The available authentication methods are Dot1x, MAB, and captive portal. Ordering sets the order of methods that the switch attempts when trying to authenticate a new device connected to a port. If one method is unsuccessful or timed out, the next method is attempted.

Each method can only be entered once. Ordering is only possible between 802.1x and MAB. Captive portal can be configured either as a stand-alone method or as the last method in the order.

Format	authentication order {dot1x [mab [captive-portal] captive-portal] mab [dot1x [captive-portal] captive-portal] captive-portal}
Mode	Interface Config

no authentication order

This command returns the port to the default authentication order.

Format	no authentication order
Mode	Interface Config

authentication priority

M4250**M4350**

This command sets the priority for the authentication methods used on a port. The available authentication methods are Dot1x, MAB, and captive portal. The authentication priority determines if a previously authenticated client is reauthenticated with a higher-priority method when another authentication request for the same client is received. Captive portal is always the last method in the list.

Default	Authentication order: dot1x, mab, captive portal
Format	authentication priority {dot1x [mab [captive portal] captive portal] mab [dot1x [captive portal] captive portal] captive portal}
Mode	Interface Config

no authentication priority

This command returns the port to the default order of priority for the authentication methods.

Format	no authentication priority
Mode	Interface Config

authentication restart

M4250**M4350**

This command sets the time, in seconds, after which reauthentication starts. The range is 300–65535 seconds and the default time is 300 seconds. The timer restarts the authentication only after all the authentication methods fail. At the expiration of this timer, authentication is reinitiated for the port.

Format	authentication restart <i>seconds</i>
Mode	Interface Config

no authentication restart

This command sets the reauthentication value to the default value of 3600 seconds.

Format	no authentication restart
Mode	Interface Config

authentication allow-unauth dhcp

M4250**M4350**

This command enables DHCP packets for unauthorized clients on the interface.

Default	Disabled
Format	<code>authentication allow-unauth dhcp</code>
Mode	Interface Config

no authentication allow-unauth dhcp

This command disables DHCP packets for unauthorized clients on the interface.

Format	<code>no authentication allow-unauth dhcp</code>
Mode	Interface Config

authentication event server dead action

M4250**M4350**

This command configures the actions that occurs when all authentication servers are “dead” (unresponsive). The command also configures the critical VLAN ID or critical voice VLAN features. If the VLAN ID is not specified, the port PVID is used as the critical VLAN ID.

Default	Action: None VLAN: Port PVID
Format	<code>authentication event server dead action {reinitialize authorize} [vlan <i>vlan-id</i> voice]</code>
Mode	Interface Config

Parameter	Definition
reinitialize	Triggers reauthentication for all authenticated clients on the port. Supplicants on the voice VLAN, unauthenticated VLAN (authentication failed clients), and guest VLAN are not disturbed. During reauthentication, if all the servers are still dead, the supplicant is authorized and placed in the critical VLAN without contacting the RADIUS server for authentication.
authorize	Authorizes the authenticated supplicants and assigns them to the critical VLAN. Supplicants on the RADIUS-assigned VLAN, voice VLAN, unauthenticated VLAN, and guest VLAN are not disturbed. Supplicants authorized on the port PVID are reauthorized on the critical VLAN.

Parameter	Definition
vlan <i>vlan id</i>	The critical VLAN ID.
voice	Enables critical voice VLAN features.

no authentication event server dead action

This command disables the dead server action.

Format	no authentication event server dead action
Mode	Interface Config

authentication event server alive action

M4250

M4350

This command configures the action that occurs when one authentication server comes back “alive” (responsive) after all were “dead” (unresponsive). The **reinitialize** action (the only possible action) triggers the reauthentication of supplicants authenticated on the critical VLAN.

Default	Action: None
Format	authentication event server alive action reinitialize
Mode	Interface Config

no authentication event server alive action

This command disables the dead server action.

Format	no authentication event server alive action
Mode	Interface Config

authentication violation

M4250

M4350

This command configures the action that occurs when a security violation occurs on a port. The authentication violation can occur when a device tries to connect to a port on which the maximum number of devices is exceeded.

Default	restrict
Format	authentication violation {protect restrict shutdown}
Mode	Interface Config
Parameter	Definition
protect	Sets the violation mode so that the port drops packets with unexpected MAC addresses without generating a system message.
restrict	Sets the violation mode so that the packets are dropped by the CPU and a system message is generated.
shutdown	Sets the violation mode so that the port is placed in the error-disabled state with unexpected MAC addresses.

no authentication violation

This command disables the authentication violation action.

Format	no authentication violation
Mode	Interface Config

authentication monitor

M4250

M4350

This command enables the authentication monitor mode on the switch. The purpose of the monitor mode is to help troubleshoot port-based authentication configuration issues without disrupting network access for hosts that are connected to the switch. In monitor mode, a host is granted network access to an authentication enforced port even if it fails the authentication process. The results of the process are logged for diagnostic purposes.

Format	authentication monitor
Mode	Global Config

no authentication monitor

This command disables the authentication monitor on the switch.

Format	no authentication monitor
Mode	Global Config

show authentication authentication-history

M4250**M4350**

Use this command to display information about the authentication history for a specified interface or for all interfaces. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show authentication authentication-history [<i>unit/slot/port</i> all]
Mode	Privileged EXEC
Term	Definition
Time Stamp	The time of the authentication.
Interface	The interface.
MAC-Address	The MAC address for the interface.
Auth Status	The authentication status for the interface.
Method	The authentication method for the interface.

Command example:

```
(NETGEAR Switch) show authentication authentication-history 0/2
```

Time Stamp	Interface	MAC-Address	Auth Status	Method
Jul 21 2020 15:06:15	1/0/1	00:00:00:00:00:01	Authorized	802.1X

show authentication

M4250**M4350**

Use this command to display authentication method information for the switch and the number of authenticated clients.

Format	show authentication
Mode	Privileged EXEC

Term	Definition
Authentication Manager Status	The authentication status on the switch (Enabled or Disabled).
Dynamic VLAN Creation Mode	Indicates if the switch can dynamically create a RADIUS-assigned VLAN if the VLAN does not exist on the switch.
VLAN Assignment Mode	Indicates if the switch can use a RADIUS-assigned VLAN in the client authentication process.
Authentication Monitor Mode	Indicates if the monitor mode is enabled on the switch.
Critical Recovery Max ReAut	The number of supplicants that can be reauthenticated per second.
Number of Authenticated clients	The total number of clients that were authenticated on the switch, except for the clients in monitor mode.
Number of clients in Monitor mode	The total number of clients that were authorized in monitor mode on the switch.

Command example:

```
(NETGEAR Switch) #show authentication
```

```
Authentication Manager Status..... Disabled
Dynamic Vlan Creation Mode..... Disabled
VLAN Assignment Mode..... Disabled
Authentication Monitor Mode..... Disabled
Critical Recovery Max ReAuth..... 10

Number of Authenticated clients..... 2
Number of clients in Monitor mode..... 0
```

show authentication interface**M4250****M4350**

Use this command to display authentication method information either for all interfaces or for a specific interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show authentication interface {all unit/slot/port}</code>
Mode	Privileged EXEC

The following information is displayed for each interface.

Term	Definition
Authentication Manager Status	The authentication status on the switch (Enabled or Disabled).
Interface	The interface for which authentication configuration information is displayed.
Port Control Mode	The control mode for the interface (force-unauthorized, auto, or unauthorized).
Host Mode	The authentication host mode on the interface.
Open Authentication	Indicates if open authentication is enabled or disabled on the interface.
Authentication Restart timer	The period in seconds, after which reauthentication starts.
Configured method order	The configured order of authentication methods on the interface.
Enabled method order	The enabled order of authentication methods on the interface.
Configured method priority	The configured priority for the authentication methods on the interface.
Enabled method priority	The enabled priority for the authentication methods on the interface.
Reauthentication Enabled	Indicates if reauthentication is enabled (TRUE) or disabled (FALSE) on the interface.
Reauthentication Session timeout from server	Indicates if, after a session time-out, client reauthentication is enabled (TRUE) or disabled (FALSE) on the interface.
Maximum Users	The maximum number of clients that can be authenticated on the interface if the interface is configured in multi-auth host mode.
Guest VLAN ID	For 802.1x unaware clients only, the VLAN ID that must be used to authorize clients that time out or fail authentication because of invalid credentials.
Authentication retry attempts	The number of reauthentication attempts that clients are allowed on the interface.
Unauthenticated VLAN ID	For 802.1x clients only, the VLAN ID that must be used to authorize clients that time out or fail authentication due to invalid credentials.
Critical Vlan Id	The VLAN ID that must be used to authorize clients that time out because RADIUS servers cannot be reached.
Authentication Violation Mode	The action that must be taken after a security violation occurs on the interface.
Authentication Server Dead action	The action that must be taken for data clients when none of the RADIUS servers can be reached.
Authentication Server Dead action for Voice	The action that must be taken for voice clients when none of the RADIUS servers can be reached.
Authentication Server Alive action	The action that must be taken for data clients when a RADIUS server becomes reachable again after none of the RADIUS servers could be reached.
Allowed protocols on unauthorized port	The protocols that are permitted on the unauthorized interface.

Command example:

```
(NETGEAR Switch) #show authentication interface 0/2
Authentication Manager Status..... Enabled

Interface..... 0/2
Port Control Mode..... auto
Host Mode..... multi-domain-multi-host
Open Authentication..... Disabled
Authentication Restart timer..... 30
Configured method order..... dot1x mab captive-portal
Enabled method order..... dot1x undefined undefined
Configured method priority..... dot1x mab captive-portal
Enabled method priority..... dot1x undefined undefined
Reauthentication Enabled..... FALSE
Reauthentication Session timeout from server .. TRUE
Maximum Users..... 48
Guest VLAN ID..... 0
Authentication retry attempts..... 3
Unauthenticated VLAN ID..... 0
Critical Vlan Id..... 0
Authentication Violation Mode..... Restrict
Authentication Server Dead action..... None
Authentication Server Dead action for Voice.... None
Authentication Server Alive action..... None
Allowed protocols on unauthorized port..... None
```

show authentication methods**M4250****M4350**

Use this command to display information about the authentication methods.

Format	show authentication methods

Mode	Privileged EXEC

Term	Definition
Authentication Login List	The authentication login listname.
Method 1	The first method in the specified authentication login list, if any.
Method 2	The second method in the specified authentication login list, if any.
Method 3	The third method in the specified authentication login list, if any.

Command example:

```
(NETGEAR Switch)#show authentication methods
```

```
Login Authentication Method Lists
```

```
-----
```

```
defaultList      : local
networkList      : local
```

```
Enable Authentication Method Lists
```

```
-----
```

```
enableList       : enable  none
enableNetList    : enable  deny
```

Line	Login Method List	Enable Method List
-----	-----	-----
Console	defaultList	enableList
Telnet	networkList	enableList
SSH	networkList	enableList

```
HTTPS           :local
HTTP            :local
DOT1X           :
```

show authentication statistics**M4250****M4350**

Use this command to display the authentication statistics for an interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show authentication statistics <i>unit/slot/port</i></code>

Mode	Privileged EXEC

The following information is displayed for each interface.

Term	Definition
Port	The port for which information is displayed.
802.1X attempts	The number of Dot1x authentication attempts for the port.
802.1X failed attempts	The number of failed Dot1x authentication attempts for the port.

Term	Definition
Mab attempts	The number of MAB (MAC authentication bypass) authentication attempts for the port.
Mab failed attempts	The number of failed MAB authentication attempts for the port.
Captive-portal attempts	The number of captive portal (Web authorization) authentication attempts for the port.
Captive-portal failed attempts	The number of failed captive portal authentication attempts for the port.

Command example:

```
(NETGEAR Switch) #show authentication statistics 0/1
```

```
Port..... 0/1
802.1X attempts..... 0
802.1X failed attempts..... 0
Mab attempts..... 0
Mab failed attempts..... 0
Captive-portal attempts..... 0
Captive-Portal failed attempts..... 0
```

show mab**M4250****M4350**

Use this command to display a summary of the MAB configuration on the switch or on a specific interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show mab [interface unit/slot/port]</code>

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show mab
```

```
MAB Request Fmt Attr1 Groupsize... 2
MAB Request Fmt Attr1 Separator... legacy(:)
MAB Request Fmt Attr1 Case..... uppercase
```

Interface	Admin Mode	Auth-type
-----	-----	-----
0/1	Disabled	N/A
0/2	Disabled	N/A
0/3	Disabled	N/A

Command example:

```
(NETGEAR Switch) #show mab interface 0/10
Interface      Admin Mode      Auth-type
0/10           Enabled      eap-md5
```

clear authentication statistics

M4250

M4350

Use this command to clear the authentication statistics on an interface or all interfaces. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	clear authentication statistics { <i>unit/slot/port</i> } all}
Mode	Privileged EXEC

clear authentication authentication-history

M4250

M4350

Use this command to clear the authentication history log for an interface or all interfaces. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	clear authentication authentication-history { <i>unit/slot/port</i> all}
Mode	Privileged EXEC

show dot1x

M4250

M4350

Use this command to display a summary of the dot1x configuration for the switch, a specific interface, or all interfaces. You can also show the detailed dot1x configuration for a specific interface or the dot1x statistics for a specific interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.

- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show dot1x [{supplicant summary {unit/slot/port all} detail unit/slot/port statistics unit/slot/port}</code>

Mode	Privileged EXEC

If you do not use the any optional parameters, the command displays the global dot1x settings for the switch.

Term	Definition
Administrative Mode	Indicates if authentication control is enabled on the switch.
EAPOL Flood Mode	Indicates if assignment of an authorized port to a RADIUS-assigned VLAN is allowed on the switch.
Software Version	The 802.1X (dot1x) firmware version on the switch.

Command example:

```
(NETGEAR Switch) #show dot1x
Administrative Mode..... Enabled
EAPOL Flood Mode..... Disabled
Software Version..... 1
```

If you use the optional parameter **supplicant summary** *{unit/slot/port | all}*, the dot1x configuration is displayed for the specified interface or, if you use the **all** parameter, for all interfaces.

Term	Definition
Interface	The interface for which the configuration is displayed.
Port Status	Indicates whether the port is authorized or unauthorized.

Command example:

```
(NETGEAR Switch) #show dot1x supplicant summary 0/1
Supplicant summary 0/1.
Operating
Interface Port Status
-----
0/1      Authorized
```

If an interface is configured as an authenticator and you use the optional parameter **detail unit/slot/port**, the following detailed dot1x configuration for the specified interface is displayed.

Term	Definition
Port	The interface for which the configuration is displayed.
Protocol Version	The protocol version associated with the interface. The only possible value is 1, corresponding to the first version of the dot1x specification.
PAE Capabilities	The port access entity (PAE) functionality of the interface (Authenticator or Supplicant).
Quiet Period	The period in seconds during which the interface does not attempt to acquire a supplicant.
Transmit Period	The period in seconds after which the interface sends an EAPOL EAP Request/Identity frame to the supplicant.
Supplicant Timeout	The period in seconds after which the interface times out the supplicant.
Server Timeout	The period in seconds after which the interface times out the authentication server.
Maximum Request-Identities	The maximum number of times that the interface retransmits an EAPOL EAP Request/Identity frame before timing out a supplicant.
Maximum Requests	The maximum number of times that the interface retransmits an EAPOL EAP Request/Identity frame before restarting the authentication process.
Key Transmission Enabled	Indicates if the interface transmits the key to the supplicant.

Command example:

```
(NETGEAR Switch) #show dot1x detail 0/3
Port..... 0/3
Protocol Version..... 1
PAE Capabilities..... Authenticator
Quiet Period (secs)..... 60
Transmit Period (secs)..... 30
Supplicant Timeout (secs)..... 30
Server Timeout (secs)..... 30
Maximum Request-Identities..... 2
Maximum Requests..... 2
Key Transmission Enabled..... False
```

If an interface is configured as a supplicant and you use the optional parameter **detail** *unit/slot/port*, the following detailed dot1x configuration for the specified interface is displayed.

Term	Definition
Port	The interface for which the configuration is displayed.
Protocol Version	The protocol version associated with the interface. The only possible value is 1, corresponding to the first version of the dot1x specification.
PAE Capabilities	The port access entity (PAE) functionality of the interface (Authenticator or Supplicant).
Control Mode	The configured control mode for the interface (force-unauthorized, auto, or unauthorized).
Supplicant PAE State	The supplicant PAE state on the interface (Initialize, Logoff, Held, Unauthenticated, Authenticating, or Authenticated.).
Maximum Start Messages	The maximum number of EAP Start messages that the supplicant sends before entering the Unauthenticated state.
Start Period	The period between each EAP Start message that the supplicant sends if the authenticator does not respond.
Held Period	The period that the interface waits before it sends authentication credentials after an earlier attempt failed.
Authentication Period	The period after which the interface times out an authenticator while waiting for a response to packets other than EAPOL-Start packets.

Command example:

```
(NETGEAR Switch) #show dot1x detail 0/4
Port..... 0/4
Protocol Version..... 1
PAE Capabilities..... Supplicant
Control Mode..... auto
Supplicant PAE State..... Authenticated
Maximum Start Messages..... 3
Start Period (secs)..... 30
Held Period (secs)..... 60
Authentication Period (secs)..... 30
```

If you use the optional parameter **statistics** *unit/slot/port*, the following dot1x statistics display for the specified interface.

Term	Definition
Port	The interface for which the statistics are displayed.
PAE Capabilities	The port access entity (PAE) functionality of the interface (Authenticator or Supplicant).
EAPOL Frames Received	The number of EAPOL frames of any type that the interface received.

Term	Definition
EAPOL Frames Transmitted	The number of EAPOL frames of any type that the interface transmitted.
EAPOL Start Frames Received	The number of EAPOL start frames that the interface received.
EAPOL Logoff Frames Received	The number of EAPOL logoff frames that the interface received.
EAP Response/Id Frames Received	The number of EAP response/identity frames that the interface received.
EAP Response Frames Received	The number of valid EAP response frames (other than response/identity frames) that the interface received.
EAP Request/Id Frames Transmitted	The number of EAP request/identity frames that the interface transmitted.
EAP Request Frames Transmitted	The number of EAP request frames (other than request/identity frames) that the interface transmitted.
Invalid EAPOL Frames Received	The number of EAPOL frames that the interface received for which the frame type was not recognized.
EAP Length Error Frames Received	The number of EAP frames that the interface received for which an invalid packet body length was detected.
Last EAPOL Frame Version	The protocol version number carried in the most recently received EAPOL frame.
Last EAPOL Frame Source	The source MAC address carried in the most recently received EAPOL frame.

Command example:

```
(NETGEAR Switch) #show dot1x statistics 0/1
Port..... 0/1
EAPOL Frames Received..... 0
EAPOL Frames Transmitted..... 0
EAPOL Start Frames Transmitted..... 3
EAPOL Logoff Frames Received..... 0
EAP Resp/Id frames transmitted..... 0
EAP Response frames transmitted..... 0
EAP Req/Id frames transmitted..... 0
EAP Req frames transmitted..... 0
Invalid EAPOL frames received..... 0
EAP length error frames received..... 0
Last EAPOL Frame Version..... 0
Last EAPOL Frame Source..... 00:00:00:00:02:01
```

show authentication clients

M4250

M4350

This command displays authentication information for clients that are authenticated on a specific interface or on all interfaces. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show authentication clients {unit/slot/port all}</code>
Mode	Privileged EXEC
Term	Definition
Interface	The interface for which the authentication configuration information is displayed.
Mac Address	The MAC address of the client.
User Name	The user name that is associated with the client.
VLAN Assigned Reason	One of the following reasons why the VLAN was assigned: • Default VLAN. The client was authenticated on the default VLAN for the interface and the authentication server is not a RADIUS server. • RADIUS. The authentication server is a RADIUS server. • Voice VLAN. The client is a voice device. • Critical VLAN. The client was authenticated on the critical VLAN. • Unauthenticated VLAN. The client was authenticated on the unauthenticated VLAN. • Guest VLAN. The client was authenticated on the guest VLAN. • Monitor Mode. The client was authenticated through the monitor mode.
Host Mode	The authentication host mode on the interface (multi-auth, multi-domain, multi-host, single-host, or multi-domain-multi-host).
Method	The method that is used to authenticate the client on the interface (802.1x, MAB, Captive Portal, or None).
Control Mode	The control mode for the interface (force-unauthorized, auto, or unauthorized).
Session time	The period the client session is active.
Session timeout	The period after which the session times out. The period in seconds is returned by the RADIUS server when authentication occurs.
Session Termination Action	This action that occurs when the session time-out expires: • Default. The session is terminated and the client details are cleared. • Radius-Request. The client is reauthenticated.
Filter-Id	The identifier that is returned by the RADIUS server when the client is authenticated. This is a configured DiffServ policy name on the switch.
DACL	The downloadable ACL that is returned by the RADIUS server when the client is authenticated.

Term	Definition
Redirect ACL	The redirect ACL is a static ACL that is sent in the RADIUS attribute redirect-acl. It is used to redirect matching packets for further action.
Redirect URL	The redirect URL is a URL that is sent in the RADIUS attribute redirect-url. It is used to redirect matching packets to the URL by using HTTP 302 response code.
Session Termination Action	This action that occurs when the session time-out expires: • Default. The session is terminated and the client details are cleared. • Radius-Request. The client is reauthenticated.
Acct SessionId	The accounting session identifier that is associated with the client session.

Command example:

```
(NETGEAR Switch) #show authentication clients 1/0/2
```

```
Mac Address..... 58:05:94:1C:00:00
User Name..... testixia
VLAN Assigned Reason..... Voice VLAN (100)
Host Mode ..... multi-auth
Method..... 802.1X
Control Mode..... auto
Session time ... 0
Session timeout ..... 0
Session Termination Action..... Default
Filter-Id ..... None
DACL..... None
Redirect ACL..... IP-REDIRECT-IN-00000001#d
Redirect URL..... http://netgear.com:8080
Session Termination Action..... Default
Acct SessionId:..... testixia:200000003
```

Command example:

```
(NETGEAR Switch) (Interface 1/0/10)#show authentication clients all
```

Interface	MAC-Address	Method	Host Mode	Control Mode	VLAN Assigned Reason
0/12	10:8D:B6:C6:00:00	802.1X	multi-host	auto	RADIUS Assigned VLAN (10)

show dot1x users

M4250

M4350

This command displays 802.1X port security user information for locally configured users. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.

- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show dot1x users <i>unit/slot/port</i></code>

Mode	Privileged EXEC

Term	Definition

Users	Users configured locally to have access to the specified port.

Command example:

```
(NETGEAR Switch) #show dot1x users 0/12
```

```
Users
```

```
-----
```

```
admin
```

```
guest
```

```
test4
```

Storm-Control Commands

This section describes commands you use to configure storm-control and view storm-control configuration information. A traffic storm is a condition that occurs when incoming packets flood the LAN, which creates performance degradation in the network. The Storm-Control feature protects against this condition.

The switch provides broadcast, multicast, and unicast storm recovery for individual interfaces. Unicast Storm-Control protects against traffic whose MAC addresses are not known by the system. For broadcast, multicast, and unicast storm-control, if the rate of traffic entering an interface increases beyond the configured threshold for that type, the traffic is dropped.

To configure storm-control, you will enable the feature for all interfaces or for individual interfaces, and you will set the threshold (storm-control level) beyond which the broadcast, multicast, or unicast traffic will be dropped. The Storm-Control feature allows you to limit the rate of specific types of packets through the switch on a per-port, per-type, basis.

Configuring a storm-control level also enables that form of storm-control. Disabling a storm-control level (using the `no` version of the command) sets the storm-control level back to the default value and disables that form of storm-control. Using the `no` version of a storm-control command (not stating a level) disables that form of storm-control but maintains the configured level (to be active the next time that form of storm-control is enabled.)

Note: The actual rate of ingress traffic required to activate storm-control is based on the size of incoming packets and the hard-coded average packet size of 512 bytes - used to calculate a packet-per-second (pps) rate - as the forwarding-plane requires pps versus an absolute rate kbps. For example, if the configured limit is 10 percent, this is converted to ~25000 pps, and this pps limit is set in forwarding plane (hardware). You get the approximate desired output when 512 bytes packets are used.

storm-control broadcast

M4250

M4350

Use this command to enable broadcast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, broadcast storm recovery is active and, if the rate of L2 broadcast traffic entering an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default	Enabled
Format	<code>storm-control broadcast</code>
Mode	Global Config Interface Config

no storm-control broadcast

Use this command to disable broadcast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format	<code>no storm-control broadcast</code>
Mode	Global Config Interface Config

storm-control broadcast action

M4250

M4350

This command configures the broadcast storm recovery action to either shut down or send traps for one, several, or all interfaces. If you enter the command in Global Config mode, the action applies to all interfaces. If you enter the command in Interface Config mode, the action applies to one or more interfaces.

If you specify the **shutdown** keyword, the interface that receives the broadcast packets at a rate above the threshold is diagnostically disabled. If you specify the **trap** keyword, the interface sends trap messages approximately every 30 seconds until broadcast storm control recovers.

Format	<code>storm-control broadcast action {shutdown trap}</code>
Mode	Global Config Interface Config

no storm-control broadcast action

This command sets the broadcast storm recovery action to the default value for one, several, or all interfaces. If you enter the command in Global Config mode, the action applies to all interfaces. If you enter the command in Interface Config mode, the action applies to one or more interfaces.

Format	<code>no storm-control broadcast action</code>
Mode	Global Config Interface Config

storm-control broadcast level

M4250

M4350

Use this command to configure the broadcast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed and enable broadcast storm recovery. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic entering an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold. The threshold level can be in the range from 0–100. The default is 5.

Default	5
Format	<code>storm-control broadcast level <i>threshold</i></code>
Mode	Global Config Interface Config

no storm-control broadcast level

This command sets the broadcast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables broadcast storm recovery.

Format	no storm-control broadcast level

Mode	Global Config Interface Config

storm-control broadcast rate

M4250

M4350

Use this command to configure the broadcast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic entering an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold. The threshold rate can be in the range from 0–14880000. The default is 0.

Default	0

Format	storm-control broadcast rate <i>threshold</i>

Mode	Global Config Interface Config

no storm-control broadcast rate

This command sets the broadcast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables broadcast storm recovery.

Format	no storm-control broadcast rate

Mode	Global Config Interface Config

storm-control multicast

M4250

M4350

This command enables multicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic entering an interface increases

beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	Disabled
Format	<code>storm-control multicast</code>
Mode	Global Config Interface Config

`no storm-control multicast`

This command disables multicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format	<code>no storm-control multicast</code>
Mode	Global Config Interface Config

`storm-control multicast action`

M4250

M4350

This command configures the multicast storm recovery action to either shut down or send traps for one, several, or all interfaces. If you enter the command in Global Config mode, the action applies to all interfaces. If you enter the command in Interface Config mode, the action applies to one or more interfaces.

If you specify the **shutdown** keyword, the interface that receives the multicast packets at a rate above the threshold is diagnostically disabled. If you specify the **trap** keyword, the interface sends trap messages approximately every 30 seconds until multicast storm control recovers.

Format	<code>storm-control multicast action {shutdown trap}</code>
Mode	Global Config Interface Config

`no storm-control multicast action`

This command sets the multicast storm recovery action to the default value for one, several, or all interfaces. If you enter the command in Global Config mode, the action applies to all interfaces. If you enter the command in Interface Config mode, the action applies to one or more interfaces.

Format	<code>no storm-control multicast action</code>

Mode	Global Config Interface Config

storm-control multicast level

M4250

M4350

This command configures the multicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic entering an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold. The threshold level can be in the range from 0–100. The default is 5.

Default	5

Format	<code>storm-control multicast level 0-100</code>

Mode	Global Config Interface Config

no storm-control multicast level

This command sets the multicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables multicast storm recovery.

Format	<code>no storm-control multicast level</code>

Mode	Global Config Interface Config

storm-control multicast rate

M4250

M4350

Use this command to configure the multicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 broadcast traffic entering an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold. The threshold rate can be in the range from 0–14880000. The default is 0.

Default	0
Format	<code>storm-control multicast rate <i>threshold</i></code>
Mode	Global Config Interface Config

no storm-control multicast rate

This command sets the multicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables multicast storm recovery.

Format	<code>no storm-control multicast rate</code>
Mode	Global Config Interface Config

storm-control unicast

M4250

M4350

This command enables unicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic entering an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default	Disabled
Format	<code>storm-control unicast</code>
Mode	Global Config Interface Config

no storm-control unicast

This command disables unicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format	<code>no storm-control unicast</code>
Mode	Global Config Interface Config

storm-control unicast action

M4250**M4350**

This command configures the unicast storm recovery action to either shut down or send traps for one, several, or all interfaces. If you enter the command in Global Config mode, the action applies to all interfaces. If you enter the command in Interface Config mode, the action applies to or one or more interfaces.

If you specify the **shutdown** keyword, the interface that receives the unicast packets at a rate above the threshold is diagnostically disabled. If you specify the **trap** keyword, the interface sends trap messages approximately every 30 seconds until unicast storm control recovers.

Format	storm-control unicast action {shutdown trap}

Mode	Global Config Interface Config

no storm-control unicast action

This command sets the unicast storm recovery action to the default value for one, several, or all interfaces. If you enter the command in Global Config mode, the action applies to all interfaces. If you enter the command in Interface Config mode, the action applies to or one or more interfaces.

Format	no storm-control unicast action

Mode	Global Config Interface Config

storm-control unicast level

M4250**M4350**

This command configures the unicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed, and enables unicast storm recovery. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic entering an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold. This command also enables unicast storm recovery mode for an interface. The threshold level can be in the range from 0–100. The default is 5.

Default	5
Format	<code>storm-control unicast level <i>threshold</i></code>
Mode	Global Config Interface Config

no storm-control unicast level

This command sets the unicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables unicast storm recovery.

Format	<code>no storm-control unicast level</code>
Mode	Global Config Interface Config

storm-control unicast rate

M4250

M4350

Use this command to configure the unicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, unicast storm recovery is active, and if the rate of L2 broadcast traffic entering an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unicast traffic is limited to the configured threshold. The threshold rate can be in the range from 0–14880000. The default is 0.

Default	0
Format	<code>storm-control unicast rate <i>threshold</i></code>
Mode	Global Config Interface Config

no storm-control unicast rate

This command sets the unicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables unicast storm recovery.

Format	<code>no storm-control unicast rate</code>
Mode	Global Config Interface Config

show storm-control

M4250

M4350

This command displays switch configuration information. If you do not use any of the optional parameters, this command displays global storm control configuration parameters:

- **Broadcast Storm Recovery Mode** may be enabled or disabled. The factory default is disabled.
- **802.3x Flow Control Mode** may be enabled or disabled. The factory default is disabled.

Use the **all** keyword to display the per-port configuration parameters for all interfaces. To specify a specific interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format show storm-control [all | unit/slot/port]

Mode Privileged EXEC

Parameter	Definition
Bcast Mode	Shows whether the broadcast storm control mode is enabled or disabled. The factory default is disabled.
Bcast Level	The broadcast storm control level.
Bcast Action	The broadcast storm recovery action.
Mcast Mode	Shows whether the multicast storm control mode is enabled or disabled.
Mcast Level	The multicast storm control level.
Mcast Action	The multicast storm recovery action.
Ucast Mode	Shows whether the Unknown Unicast or DLF (Destination Lookup Failure) storm control mode is enabled or disabled.
Ucast Level	The Unknown Unicast or DLF (Destination Lookup Failure) storm control level.
Ucast Action	The unicast storm recovery action.

Command example:

```
(NETGEAR Switch) #show storm-control
```

```
Broadcast Storm Control Mode..... Enable
Broadcast Storm Control Level..... 5 percent
Broadcast Storm Control Action..... None
Multicast Storm Control Mode..... Disable
Multicast Storm Control Level..... 5 percent
```



```

Multicast Storm Control Action..... None
Unicast Storm Control Mode..... Disable
Unicast Storm Control Level..... 5 percent
Unicast Storm Control Action..... None

```

Command example:

```
(NETGEAR Switch) #show storm-control 1/0/1
```

Bcast Intf	Bcast Mode	Bcast Level	Mcast Action	Mcast Mode	Mcast Level	Ucast Action	Ucast Mode	Ucast Level	Flow Action	Mode
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----
1/0/1	Enable	5%	None	Disable	5%	None	Disable	5%	None	Disable

Command example:

```
(NETGEAR Switch) #show storm-control all
```

Bcast Intf	Bcast Mode	Bcast Level	Mcast Action	Mcast Mode	Mcast Level	Ucast Action	Ucast Mode	Ucast Level	Flow Action	Mode
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----
1/0/1	Enable	5%	None	Disable	5%	None	Disable	5%	None	Disable
1/0/2	Enable	5%	None	Disable	5%	None	Disable	5%	None	Disable
1/0/3	Enable	5%	None	Disable	5%	None	Disable	5%	None	Disable
1/0/4	Enable	5%	None	Disable	5%	None	Disable	5%	None	Disable
1/0/5	Enable	5%	None	Disable	5%	None	Disable	5%	None	Disable

Link Dependency Commands

Link dependency allows the link status of specified ports to be dependent on the link status of one port or many ports. Consequently, if a port on which other ports depend loses a link, the dependent ports either become administratively disabled and are brought down or become administratively enabled and are brought up.

link state group action

M4250

M4350

Use this command to indicate if the downstream interfaces of a specified group must mirror or invert the status of the upstream interfaces. The default configuration for a group is down. That is, the downstream interfaces mirror the upstream link status by going down when all upstream interfaces are down. Specifying the **up** keyword allows the downstream interfaces to come up when all upstream interfaces are down.

Default	down
Format	link state group <i>group-id</i> action {up down}
Mode	Global Config

no link state group action

Use this command to reset the link state action for downstream interfaces to the default action (down).

Format	no link state group <i>group-id</i> action
Mode	Global Config

link state group downstream

M4250

M4350

Use this command to add a group of interfaces to the downstream interface list. Adding an interface to a downstream list brings the interface down until an upstream interface is added to the group. The link status then follows the interface that is specified in the **link state group upstream** command. To prevent interfaces from being brought down, enter the **link state group upstream** command before you enter the **link state group downstream** command.

Format	link state group <i>group-id</i> downstream
Mode	Interface Config

no link state group downstream

Use this command to remove a group of interfaces from the downstream list.

Format	no link state group <i>group-id</i> downstream
Mode	Interface Config

link state group upstream

M4250**M4350**

Use this command to add a group of interfaces to the upstream interface list.

An interface that is defined as an upstream interface cannot also be defined as a downstream interface in the same link state group or as a downstream interface in a different link state group if either configuration creates a circular dependency between groups.

Format	link state group <i>group-id</i> upstream

Mode	Interface Config

no link state group upstream

Use this command to remove a group of interfaces from the upstream list.

Format	no link state group <i>group-id</i> upstream

Mode	Interface Config

show link state group

M4250**M4350**

Use this command to display information about all configured link-dependency groups or a specific link-dependency group.

Format	show link state group [<i>group-id</i>]

Mode	Privileged EXEC

Command example:

This example displays information about all configured link-dependency groups.

```
(Switching) #show link-state group
```

GroupId	Downstream Interfaces	Upstream Interfaces	Link Action	Group State
-----	-----	-----	-----	-----
1	2/0/3-2/0/7,2/0/12-2/0/17	2/0/12-2/0/32,0/3/5	Link Up	Up
4	2/0/18,2/0/27	2/0/22-2/0/33,0/3/1	Link Up	Down

Command example:

This example displays information about a specific link-dependency group.

```
(Switching) #show link state group 1
```

GroupId	Downstream Interfaces	Upstream Interfaces	Link Action	Group State
-----	-----	-----	-----	-----
1	2/0/3-2/0/7,2/0/12-2/0/17	2/0/12-2/0/32,0/3/5	Link Up	Up

show link state group detail

M4250**M4350**

Use this command to display detailed information about the state of upstream and downstream interfaces for a selected link-dependency group. The Group Transitions field shows a count of the number of times that the downstream interface went into its action state as a result of the upstream interfaces link state.

Format	show link state group <i>group-id</i> detail
Mode	Privileged EXEC

Command example:

```
(Switching) #show link state group 1 detail
GroupId:      1
Link Action:  Up
Group State:  Up

Downstream Interface State:
Link Up:      2/0/3
Link Down:    2/0/4-2/0/7,2/0/12-2/0/17

Upstream Interface State:
Link Up:      -
Link Down:    2/0/12-2/0/32,0/3/5

Group Transitions: 0
Last Transition Time: 00:52:35 (UTC+0:00) Nov 3 2015
```

Link Local Protocol Filtering Commands

Link Local Protocol Filtering (LLPF) allows the switch to filter out multiple proprietary protocol PDUs, such as Port Aggregation Protocol (PAgP), if the problems occur with proprietary protocols running on standards-based switches. If certain protocol PDUs cause unexpected results, LLPF can be enabled to prevent those protocol PDUs from being processed by the switch.

llpf

M4250

M4350

Use this command to block LLPF protocol(s) on a port.

Default	disable
Format	llpf {blockisdp blockvtp blockdtp blockudld blockpagp blocksstp blockall}
Mode	Interface Config

no llpf

Use this command to unblock LLPF protocol(s) on a port.

Format	no llpf {blockisdp blockvtp blockdtp blockudld blockpagp blocksstp blockall }
Mode	Interface Config

show llpf interface

M4250

M4350

Use this command to display the status of LLPF rules configured on a particular port or on all ports. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show llpf interface [all unit/slot/port]
Mode	Privileged EXEC

Term	Definition
Block ISDP	Shows whether the port blocks ISDP PDUs.
Block VTP	Shows whether the port blocks VTP PDUs.
Block DTP	Shows whether the port blocks DTP PDUs.
Block UDLD	Shows whether the port blocks UDLD PDUs.
Block PAGP	Shows whether the port blocks PAGP PDUs.
Block SSTP	Shows whether the port blocks SSTP PDUs.
Block All	Shows whether the port blocks all proprietary PDUs available for the LLDP feature.

Port-Channel/LAG (802.3ad) Commands

This section describes the commands you use to configure port-channels, which is defined in the 802.3ad specification, and that are also known as link aggregation groups (LAGs). Link aggregation allows 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. The LAG feature initially load shares traffic based upon the source and destination MAC address. Assign the port-channel (LAG) VLAN membership after you create a port-channel. If you do not assign VLAN membership, the port-channel might become a member of the management VLAN which can result in learning and switching issues.

A port-channel interface, also referred to as a link aggregation group (LAG) or an EtherChannel, can be either static or dynamic, but not both. All members of a port channel 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.

Note: If you configure the maximum number of dynamic port-channels (LAGs) that your platform supports, additional port-channels that you configure are automatically static.

port-channel auto

M4250

M4350

This command globally enables the Auto-LAG feature. An Auto-LAG is a LAG that can form automatically between two devices that support the Auto-LAG feature. An Auto-LAG is a dynamic Layer 2 LAG that is based on the Link Aggregation Control Protocol (LACP).

The switch can detect the physical links with a partner device and automatically configure a LAG (that is, an Auto-LAG) on interconnected and capable ports at both ends. The switch can form one Auto-LAG only with each partner device.

Both the Auto-LAG and Auto-Trunk features must be supported and globally enabled on the switch and the partner device. At least two links must be established between the switch and the partner device, and these links must be in the default switch port mode and support the same speed and duplex mode.

Default	Enabled
Format	<code>port-channel auto</code>
Mode	Global Config

`no port-channel auto`

This command globally disables the Auto-LAG feature.

Format	<code>no port-channel auto</code>
Mode	Global Config

`port-channel auto load-balance` (M4250 series switch)

M4250

This command globally configures the hash mode for load-balancing on Auto-LAGs.

Default	2
Format	<code>port-channel auto load-balance {1 2 3 4 5 6}</code>
Mode	Global Config

Term	Definition
1	Source MAC, VLAN, EtherType, and incoming port associated with the packet
2	Destination MAC, VLAN, EtherType, and incoming port associated with the packet
3	Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet
4	Source IP and Source TCP/UDP Port fields of the packet
5	Destination IP and Destination TCP/UDP Port fields of the packet
6	Source/Destination IP and source/destination TCP/UDP Port fields of the packet

no port-channel auto load-balance (M4250 series switch)

This globally command configures the default hash value (2) for load-balancing on Auto-LAGs.

Format	no port-channel auto load-balance
Mode	Global Config

port-channel auto load-balance (M4350 series switch)

M4350

This command globally configures the hash mode for load-balancing on Auto-LAGs.

Default	2
Format	port-channel auto load-balance {1 2 3 4 5 6 7}
Mode	Global Config

Term	Definition
1	Source MAC, VLAN, EtherType, and incoming port associated with the packet
2	Destination MAC, VLAN, EtherType, and incoming port associated with the packet
3	Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet
4	Source IP and Source TCP/UDP Port fields of the packet
5	Destination IP and Destination TCP/UDP Port fields of the packet
6	Source/Destination IP and source/destination TCP/UDP Port fields of the packet
7	Enhanced hashing mode

no port-channel auto load-balance (M4350 series switch)

This globally command configures the default hash value (2) for load-balancing on Auto-LAGs.

Format	no port-channel auto load-balance
Mode	Global Config

port-channel auto avb-profile

M4250

M4350

This command globally configures the AVB profile mode for all Auto-LAGs.

Default	Disabled
Format	port-channel auto avb-profile
Mode	Global Config

no port-channel auto avb-profile

This globally command disables the AVB profile mode for all Auto-LAGs..

Format	no port-channel auto avb-profile
Mode	Global Config

show port-channel auto

M4250

M4350

This command displays information for either all LAGs on which the Auto-LAG feature is enabled or a select LAG on which the Auto-LAG feature is enabled.

Format	show port-channel auto {all lag-intf-num}
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch)#show port-channel auto all
```

```
Auto LAG Admin Mode..... Enabled
Auto LAG Global Hash Mode..... 2
```

Log. Intf	Channel Name	Min	Link	Admin Mode	Load Type	Balance	Mbr Ports	Device/ Timeout	Port Speed	Port Active
lag 1	chl	2	Up	En.	auto	2	0/6	actor/long	Auto	True
							0/10	partner/long	Auto	True
								actor/long	Auto	True
								partner/long	Auto	True
								partner/long	Auto	True

Command example:

```
(NETGEAR Switch)#show port-channel auto 1

Auto LAG Admin Mode..... Enabled

Local Interface..... lag 1
Channel Name..... chl
Link State..... Up
Admin Mode..... Enabled
Type..... auto
Port-channel Min-links..... 2
Load Balance Option..... 2
(Dest MAC, VLAN, EType, incoming port)

Mbr      Device/      Port      Port
Ports    Timeout      Speed      Active
-----  -
0/6      actor/long      Auto      True
         partner/long
0/10     actor/long      Auto      True
         partner/long
```

port-channel name

M4250

M4350

This command configures a new port-channel (LAG) and generates a logical number for the port-channel.

The *name* field is a character string which allows the dash “-” character as well as alphanumeric characters. Use the **show port channel** command to display the number for the logical interface.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

You can also use **lag lag-intf-num** to specify the LAG interface, in which *lag-intf-num* is the LAG port number.

Note: Before you include a port in a port-channel, set the port physical mode. For more information, see [speed on page 485](#).

Format	<code>port-channel [unit/slot/port lag lag-intf-num] name</code>

Mode	Global Config

no port-channel name

Use this command removes a port channel and the associated name.

Format	<code>no port-channel [unit/slot/port lag lag-intf-num]</code>

Mode	Global Config

addport

M4250

M4350

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

This command adds one port to the port-channel (LAG). The first interface is a logical number of a configured port-channel. You can add a range of ports by specifying the port range when you enter Interface Config mode (for example: **interface 1/0/1-1/0/4**). You can also use **lag lag-intf-num** to specify the LAG interface, in which *lag-intf-num* is the LAG port number.

Note: Before adding a port to a port-channel, set the physical mode of the port. For more information, see [speed on page 485](#).

Format	<code>addport unit/slot/port</code>

Mode	Interface Config

deleteport (Interface Config)

M4250

M4350

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

This command deletes a port or a range of ports from the port-channel (LAG). The interface is a logical *unit/slot/port* number of a configured port-channel (or range of port-channels). Instead of *unit/slot/port*, **lag** *lag-intf-num* can be used as an alternate way to specify the LAG interface, in which *lag-intf-num* is the LAG port number.

Format	<code>deleteport unit/slot/port</code>

Mode	Interface Config

deleteport (Global Config)

M4250

M4350

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

This command deletes all configured ports from the port-channel (LAG). The interface is a logical *unit/slot/port* number of a configured port-channel. Instead of *unit/slot/port*, **lag** *lag-intf-num* can be used as an alternate way to specify the LAG interface, in which *lag-intf-num* is the LAG port number.

Format	<code>deleteport {unit/slot/port all}</code>

Mode	Global Config

lacp admin key

M4250

M4350

Use this command to configure the administrative value of the key for the port-channel. The range for *key* is 0 to 65535.

Default	0x8000

Format	<code>lacp admin key key</code>

Mode	Interface Config

Note: This command is applicable only to port-channel interfaces.

This command can be used to configure a single interface or a range of interfaces.

no lacp admin key

Use this command to configure the default administrative value of the key for the port-channel.

Format	no lacp admin key

Mode	Interface Config

lacp collector max-delay

M4250

M4350

Use this command to configure the port-channel collector max delay. This command can be used to configure a single interface or a range of interfaces. The range of *delay* is 0-65535.

Default	0x8000

Format	lacp collector max delay <i>delay</i>

Mode	Interface Config

Note: This command is applicable only to port-channel interfaces.

no lacp collector max delay

Use this command to configure the default port-channel collector max delay.

Format	no lacp collector max delay

Mode	Interface Config

lacp actor admin key

M4250

M4350

Use this command to configure the administrative value of the LACP actor admin key on an interface or range of interfaces. The range for *key* is 0-65535.

Default	Internal Interface Number of this Physical Port

Format	lacp actor admin key <i>key</i>

Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp actor admin key

Use this command to configure the default administrative value of the key.

Format	no lacp actor admin key

Mode	Interface Config

lacp actor admin state

M4250

M4350

Use this command to configure the administrative value of the actor state in LACPDUs. You can set the state to individual, long time-out, or passive. You can use this command to configure a single interface or a range of interfaces.

Default	0x07

Format	lacp actor admin state {individual longtimeout passive}

Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp actor admin state

Use this command to configure the default administrative values of the actor state in LACPDUs.

Note: Both the **no portlacptimeout** and the **no lacp actor admin state** commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands display in the output of the **show running-config** command.

Format	no lacp actor admin state {individual longtimeout passive}

Mode	Interface Config

lacp actor port priority

M4250**M4350**

Use this command to configure the priority value assigned to the aggregation port for an interface or range of interfaces. The valid range for *priority* is 0 to 65535.

Default	0x80
Format	<code>lacp actor port priority <i>priority</i></code>
Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp actor port priority

Use this command to configure the default priority value assigned to the aggregation port.

Format	<code>no lacp actor port priority</code>
Mode	Interface Config

lacp partner admin key

M4250**M4350**

Use this command to configure the administrative value of the Key for the protocol partner. This command can be used to configure a single interface or a range of interfaces. The valid range for *key* is 0 to 65535.

Default	0x0
Format	<code>lacp partner admin key <i>key</i></code>
Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner admin key

Use this command to set the administrative value of the key for the protocol partner to the default.

Format	no lacp partner admin key

Mode	Interface Config

lacp partner admin state individual

M4250

M4350

Use this command to set LACP partner admin state to individual.

Format	lacp partner admin state individual

Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner admin state individual

Use this command to set the LACP partner admin state to aggregation.

Format	no lacp partner admin state individual

Mode	Interface Config

lacp partner admin state longtimeout

M4250

M4350

Use this command to set LACP partner admin state to long time-out.

Format	lacp partner admin state longtimeout

Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner admin state longtimeout

Use this command to set the LACP partner admin state to short time-out.

Format	no lacp partner admin state longtimeout

Mode	Interface Config

Note: This command is applicable only to physical interfaces.

lacp partner admin state passive

M4250

M4350

Use this command to set the LACP partner admin state to passive.

Format	lacp partner admin state passive

Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner admin state passive

Use this command to set the LACP partner admin state to active.

Format	no lacp partner admin state passive

Mode	Interface Config

lacp partner port id

M4250

M4350

Use this command to configure the LACP partner port id. This command can be used to configure a single interface or a range of interfaces. The valid range for *port-id* is 0 to 65535.

Default	0x80

Format	lacp partner port-id <i>port-id</i>

Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner port id

Use this command to set the LACP partner port id to the default.

Format	no lacp partner port-id

Mode	Interface Config

lacp partner port priority

M4250

M4350

Use this command to configure the LACP partner port priority. This command can be used to configure a single interface or a range of interfaces. The valid range for *priority* is 0 to 65535.

Default	0x0

Format	lacp partner port priority <i>priority</i>

Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner port priority

Use this command to configure the default LACP partner port priority.

Format	no lacp partner port priority

Mode	Interface Config

lacp partner system id

M4250

M4350

Use this command to configure the 6-octet MAC Address value representing the administrative value of the Aggregation Port's protocol Partner's System ID. This command can be used to configure a single interface or a range of interfaces. The valid range of *system-id* is 00:00:00:00:00:00 - FF:FF:FF:FF:FF:FF.

Default	00:00:00:00:00:00

Format	lacp partner system id <i>system-id</i>

Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner system id

Use this command to configure the default value representing the administrative value of the Aggregation Port's protocol Partner's System ID.

Format	no lacp partner system id

Mode	Interface Config

lacp partner system priority

M4250

M4350

Use this command to configure the administrative value of the priority associated with the Partner's System ID. This command can be used to configure a single interface or a range of interfaces. The valid range for *priority* is 0 to 65535.

Default	0x0

Format	lacp partner system priority <i>priority</i>

Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner system priority

Use this command to configure the default administrative value of priority associated with the Partner's System ID.

Format	no lacp partner system priority

Mode	Interface Config

interface lag

M4250**M4350**

Use this command to enter Interface configuration mode for the specified LAG.

Format	<code>interface lag lag-interface-number</code>
Mode	Global Config

port-channel static

M4250**M4350**

This command enables the static mode on a port-channel (LAG) interface or range of interfaces. By default the static mode for a new port-channel is enabled, which means the port-channel is static. If the maximum number of allowable dynamic port-channels are already present in the system, the static mode for a new port-channel is enabled, which means the port-channel is static. You can only use this command on port-channel interfaces.

Default	Disabled
Format	<code>port-channel static</code>
Mode	Interface (LAG) Config

no port-channel static

This command sets the static mode on a particular port-channel (LAG) interface to the default value. This command will be executed only for interfaces of type port-channel (LAG).

Format	<code>no port-channel static</code>
Mode	Interface (LAG) Config

port lacpmode

M4250**M4350**

This command enables Link Aggregation Control Protocol (LACP) on a port or range of ports.

Default	Enabled
Format	<code>port lacpmode</code>
Mode	Interface Config

no port lacpmode

This command disables Link Aggregation Control Protocol (LACP) on a port.

Format	no port lacpmode

Mode	Interface Config

port lacpmode enable all

M4250

M4350

This command enables Link Aggregation Control Protocol (LACP) on all ports.

Format	port lacpmode enable all

Mode	Global Config

no port lacpmode enable all

This command disables Link Aggregation Control Protocol (LACP) on all ports.

Format	no port lacpmode enable all

Mode	Global Config

port lacptimeout (Interface Config)

M4250

M4350

This command sets the time-out on a physical interface or range of interfaces of a particular device type (actor or partner) to either long (90 seconds) or short (3 seconds) time-out.

Default	long

Format	port lacptimeout {actor partner} {long short}

Mode	Interface Config

no port lacptimeout

This command sets the time-out back to a long time-out on a physical interface of a particular device type (actor or partner).

Format	no port lacptimeout {actor partner}

Mode	Interface Config

Note: Both the `no portlacptimeout` and the `no lacp actor admin state` commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands display in the output of the `show running-config` command.

port lacptimeout (Global Config)

M4250

M4350

This command sets the time-out for all interfaces of a particular device type (actor or partner) to either long (90 seconds) or short (3 seconds) time0out.

Default	long
Format	port lacptimeout {actor partner} {long short}
Mode	Global Config

no port lacptimeout

This command sets the time-out for all physical interfaces of a particular device type (actor or partner) back to a long time-out .

Format	no port lacptimeout {actor partner}
Mode	Global Config

Note: Both the `no portlacptimeout` and the `no lacp actor admin state` commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands display in the output of the `show running-config` command.

port-channel adminmode

M4250

M4350

This command enables all configured port-channels with the same administrative mode setting.

Format	port-channel adminmode all
Mode	Global Config

no port-channel adminmode

This command disables all configured port-channels with the same administrative mode setting.

Format	no port-channel adminmode all

Mode	Global Config

port-channel linktrap

M4250

M4350

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

This command enables link trap notifications for the port-channel (LAG). The interface is a logical *unit/slot/port* for a configured port-channel. The option **all** sets every configured port-channel with the same administrative mode setting. Instead of *unit/slot/port*, **lag** *lag-intf-num* can be used as an alternate way to specify the LAG interface, in which *lag-intf-num* is the LAG port number.

Default	Disabled

Format	port-channel linktrap { <i>unit/slot/port</i> all}

Mode	Global Config

no port-channel linktrap

This command disables link trap notifications for the port-channel (LAG). The interface is a logical slot and port for a configured port-channel. The option **all** sets every configured port-channel with the same administrative mode setting.

Format	no port-channel linktrap { <i>unit/slot/port</i> all}

Mode	Global Config

port-channel load-balance (M4250 series switch)

M4250

This command selects the load-balancing option 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.

Load-balancing is not supported on every device. The range of options for load-balancing may vary per device.

This command can be configured for a single interface, a range of interfaces, or all interfaces. Instead of *slot/port*, **lag** *lag-intf-num* can be used as an alternate way to specify the LAG interface, in which *lag-intf-num* is the LAG port number.

Default	3
Format	<code>port-channel load-balance {1 2 3 4 5 6} {slot/port all lag lag-int-num}</code>
Mode	Interface (LAG) Config Global Config
Term	Definition
1	Source MAC, VLAN, EtherType, and incoming port associated with the packet.
2	Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
3	Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
4	Source IP and Source TCP/UDP fields of the packet.
5	Destination IP and Destination TCP/UDP Port fields of the packet.
6	Source/Destination IP and source/destination TCP/UDP Port fields of the packet.
slot/port	Global Config Mode only: The interface is a logical slot/port number of a configured port-channel.
all	Global Config Mode only: a11 applies the command to all currently configured port-channels.
lag-int-num	Global Config Mode only: The interface is a LAG interface number.

no port-channel load-balance (M4250 series switch)

This command reverts to the default load balancing configuration.

Format	<code>no port-channel load-balance {slot/port all lag lag-int-num}</code>
Mode	Interface (LAG) Config Global Config
Term	Definition
slot/port	Global Config Mode only: The interface is a logical unit/slot/port number of a configured port-channel.
all	Global Config Mode only: a11 applies the command to all currently configured port-channels.
lag-int-num	Global Config Mode only: The interface is a LAG interface number.

port-channel load-balance (M4350 series switch)

M4350

This command selects the load-balancing option 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.

Load-balancing is not supported on every device. The range of options for load-balancing may vary per device.

This command can be configured for a single interface, a range of interfaces, or all interfaces. Instead of *unit/slot/port*, **lag** *lag-intf-num* can be used as an alternate way to specify the LAG interface, in which *lag-intf-num* is the LAG port number.

Default	3
Format	port-channel load-balance {1 2 3 4 5 6 7} {unit/slot/port all lag lag-int-num}
Mode	Interface (LAG) Config Global Config

Term	Definition
1	Source MAC, VLAN, EtherType, and incoming port associated with the packet.
2	Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
3	Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
4	Source IP and Source TCP/UDP fields of the packet.
5	Destination IP and Destination TCP/UDP Port fields of the packet.
6	Source/Destination IP and source/destination TCP/UDP Port fields of the packet.
7	Enhanced hashing mode.
unit/slot/port	Global Config Mode only: The interface is a logical unit/slot/port number of a configured port-channel.
all	Global Config Mode only: a ll applies the command to all currently configured port-channels.
lag-int-num	Global Config Mode only: The interface is a LAG interface number.

no port-channel load-balance (M4350 series switch)

This command reverts to the default load balancing configuration.

Format	no port-channel load-balance {unit/slot/port all lag lag-int-num}
Mode	Interface (LAG) Config Global Config

Term	Definition
unit/slot/port	Global Config Mode only: The interface is a logical unit/slot/port number of a configured port-channel.
all	Global Config Mode only: a11 applies the command to all currently configured port-channels.
lag-int-num	Global Config Mode only: The interface is a LAG interface number.

port-channel load-balance 0

M4250

M4350

This command selects the non-unicast global hash mode load-balancing option used on a port-channel (LAG). With this mode, you can select one, several, or all of the options from 1 to 4.

Default	2 and 3
Format	<code>port-channel load-balance 0 [1] [2] [3] [4]</code>
Mode	Global Config

Term	Definition
1	Non-unicast global hash mode that is based on the source port.
2	Non-unicast global hash mode that is based on the source MAC address and IP address.
3	Non-unicast global hash mode that is based on the destination MAC address and IP address.
4	Non-unicast global enhanced hash mode.

no port-channel load-balance 0

This command reverts to the default load balancing configuration.

Format	<code>no port-channel load-balance 0</code>
Mode	Global Config

port-channel local-preference

M4350

This command enables the local-preference mode on a port-channel (LAG) interface or range of interfaces. By default, the local-preference mode for a port-channel is disabled. This command can be used only on port-channel interfaces.

Default	Disabled
Format	port-channel local-preference
Mode	Interface (LAG) Config

no port-channel local-preference

This command disables the local-preference mode on a port-channel.

Format	no port-channel local-preference
Mode	Interface (LAG) Config

port-channel min-links

M4250**M4350**

This command configures the port-channel's minimum links value for LAG interfaces. The *number* parameter can be in the range 1–8. The default is 1.

Default	1
Format	port-channel min-links <i>number</i>
Mode	Interface (LAG) Config

no port-channel min-links

This command resets the port-channel's minimum links value for LAG interfaces to the default value of 1.

Format	no port-channel local-preference
Mode	Interface (LAG) Config

port-channel system priority

M4250**M4350**

Use this command to configure port-channel system priority. The valid range of *priority* is 0-65535.

Default	0x8000
Format	port-channel system priority <i>priority</i>
Mode	Global Config

no port-channel system priority

Use this command to configure the default port-channel system priority value.

Format	no port-channel system priority
Mode	Global Config

show lacp actor

M4250**M4350**

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Use this command to display LACP actor attributes. Instead of *unit/slot/port*, **lag** *lag-intf-num* can be used as an alternate way to specify the LAG interface, in which *lag-intf-num* is the LAG port number.

Format	show lacp actor { <i>unit/slot/port</i> all}
Mode	Global Config

The following output parameters are displayed.

Parameter	Description
System Priority	The administrative value of the Key.
Actor Admin Key	The administrative value of the Key.
Port Priority	The priority value assigned to the Aggregation Port.
Admin State	The administrative values of the actor state as transmitted by the Actor in LACPDUs.

show lacp partner

M4250

M4350

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Use this command to display LACP partner attributes. Instead of *unit/slot/port*, **lag** *lag-intf-num* can be used as an alternate way to specify the LAG interface, in which *lag-intf-num* is the LAG port number.

Format	<code>show lacp actor {unit/slot/port all}</code>
Mode	Privileged EXEC

The following output parameters are displayed.

Parameter	Description
System Priority	The administrative value of priority associated with the Partner's System ID.
System-ID	Represents the administrative value of the Aggregation Port's protocol Partner's System ID.
Admin Key	The administrative value of the Key for the protocol Partner.
Port Priority	The administrative value of the Key for protocol Partner.
Port-ID	The administrative value of the port number for the protocol Partner.
Admin State	The administrative values of the actor state for the protocol Partner.

show port-channel brief

M4250

M4350

This command displays the static capability of all port-channel (LAG) interfaces on the device as well as a summary of individual port-channel interfaces.

Format	<code>show port-channel brief</code>
Mode	User EXEC

For each port-channel the following information is displayed.

Term	Definition
Logical Interface	The details of the logical interface.
Port-channel Name	The name of port-channel (LAG) interface.
Link-State	Shows whether the link is up or down.
Trap Flag	Shows whether trap flags are enabled or disabled.
Type	Shows whether the port-channel is statically or dynamically maintained.
Mbr Ports	The members of this port-channel.
Active Ports	The ports that are actively participating in the port-channel.

show port-channel

M4250

M4350

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

This command displays the details about a specific port channel (LAG) or an overview of all port-channels on the switch.

Format	<code>show port-channel {all unit/slot/port lag-intf-num}</code>
Mode	Privileged EXEC

Term	Definition
Logical Interface	The logical interface number.
Channel Name	The name of the LAG.
Min	The minimum links value.
Link	Indicates if the link is up or down.
Admin Mode	May be enabled or disabled. The default is enabled.
Type	The status designating if a the LAG is statically or dynamically maintained. • Static. The LAG is statically maintained. • Dynamic. The LAG is dynamically maintained.
Load Balance	The load balance option associated with this LAG. See port-channel load-balance (M4350 series switch) on page 685.

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Mbr Ports	A list of the ports that are members of this LAG. A maximum of eight ports can be assigned to a LAG.
Device/Timeout	For each port, lists the time-out (long or short) for the device type (actor or partner).
Port Speed	Speed of the LAG port.
Port Active	This field lists ports that are actively participating in the LAG.

Command example:

```
(NETGEAR Switch) #show port-channel all
```

Log. Intf	Channel Name	Min	Link	Admin Mode	Load Type	Balance	Mbr Ports	Device/ Timeout	Port Speed	Port Active
lag 1	LAG1	1	Down	En.	Dyn.	3				
lag 2	ch2	1	Down	En.	Dyn.	2				
lag 3	ch3	1	Down	En.	Dyn.	2				
lag 4	ch4	1	Down	En.	Dyn.	2				
lag 5	ch5	1	Down	En.	Dyn.	2				
lag 6	ch6	1	Down	En.	Dyn.	2				
lag 7	ch7	1	Down	En.	Dyn.	2				
lag 8	ch8	1	Down	En.	Dyn.	2				
lag 9	ch9	1	Down	En.	Dyn.	2				
lag 10	ch10	1	Down	En.	Dyn.	2				
lag 11	ch11	1	Down	En.	Dyn.	2				
lag 12	ch12	1	Down	En.	Dyn.	2				
lag 13	ch13	1	Down	En.	Dyn.	2				
lag 14	ch14	1	Down	En.	Dyn.	2				
lag 15	ch15	1	Down	En.	Dyn.	2				
lag 16	ch16	1	Down	En.	Dyn.	2				

show port-channel global-load-balance

M4250

M4350

This command displays the global LAG non-unicast hash mode.

Format show port-channel global-load-balance

Mode Privileged EXEC

Command example:

```
(NETGEAR Switch)#show port-channel global-load-balance
```

```
Global Load Balance Option(s)..... 1(Source port) 2(Source MAC/IP)
3(Destination MAC/IP)
```

show port-channel system priority

M4250**M4350**

Use this command to display the port-channel system priority.

Format	show port-channel system priority
Mode	Privileged EXEC

show port-channel counters

M4250**M4350**

This command displays the port-channel counters for a specific port channel (LAG) or interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show port-channel {unit/slot/port lag-intf-num} counters
Mode	Privileged EXEC

Term	Definition
Local Interface	The details about the interface.
Channel Name	The name of this port-channel (LAG).
Link State	Indicates whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Port Channel Flap Count	The number of times the port-channel was inactive.
Mbr Ports	The unit/port for the port member.
Mbr Flap Counters	The number of times a port member is inactive, either because the link is down, or the admin state is disabled.

Command example:

```
(NETGEAR Switch) #show port-channel 3/1 counters
```

```
Local Interface..... 3/1
Channel Name..... chl
Link State..... Down
Admin Mode..... Enabled
```



```
Port Channel Flap Count..... 0
```

Mbr Ports	Mbr Flap Counters
-----	-----
0/1	0
0/2	0
0/3	1
0/4	0
0/5	0
0/6	0
0/7	0
0/8	0

clear port-channel counters

M4250

M4350

Use this command to clear and reset specified port-channel and member flap counters for a port channel or interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>clear port-channel {lag-intf-num unit/slot/port} counters</code>

Mode	Privileged EXEC

clear port-channel all counters

M4250

M4350

Use this command to clear and reset all port-channel and member flap counters for the specified interface.

Format	<code>clear port-channel all counters</code>

Mode	Privileged EXEC

Port Mirroring Commands

Port mirroring, which is also known as port monitoring, selects network traffic that you can analyze with a network analyzer, such as a SwitchProbe device or other Remote Monitoring (RMON) probe.

monitor session source

M4250

M4350

This command adds a source interface for a port mirroring session that is identified by the *session-id* argument (an integer value).

Use the **source interface** {*unit/slot/port* | *cpu* | *lag lag-group-id*} parameters to specify the interface to monitor. You can also configure a VLAN as the source for the session (all member ports of that VLAN are monitored).

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Note: If an interface is a member of both a VLAN and a LAG, you cannot assign the VLAN as a source VLAN for a monitor session. However, if an interface is a member of a VLAN and you assign the VLAN as a source VLAN for a monitor session, afterwards you can add the interface as a member to a LAG.

You can configure remote port mirroring by specifying the **remote vlan** keywords and an RSPAN VLAN ID. At the source switch, you must specify the destination as the RSPAN VLAN. At the destination switch, you must specify the source as the RSPAN VLAN. You cannot configure the source and destination as remote on the same switch.

Note: On an intermediate switch, you must create an RSPAN VLAN, make sure that the ports that are connected to the source and destination switches are members of the RSPAN VLAN, and enable RSPAN VLAN egress tagging on the port that is connected to the destination switch.

Use **rx** to monitor only ingress packets or use **tx** to monitor only egress packets. If you do not specify an **rx** or **tx** option, the destination port monitors both ingress and egress packets.

Format	<code>monitor session <i>session-id</i> source {interface {<i>unit/slot/port</i> <i>cpu</i> <i>lag lag-group-id</i>} <i>vlan vlan-id</i> <i>remote vlan vlan-id</i>} [<i>rx</i> <i>tx</i>]</code>

Mode	Global Config

no monitor session source

This command removes a source interface for a port mirroring session that is identified by the *session-id* argument (an integer value).

Format	<code>no monitor session <i>session-id</i> source {interface {<i>unit/slot/port</i> <i>cpu</i> <i>lag lag-group-id</i>} <i>vlan vlan-id</i> <i>remote vlan vlan-id</i>}</code>

Mode	Global Config

monitor session destination

M4250

M4350

This command adds a destination interface for a port mirroring session that is identified by the *session-id* argument (an integer value).

Use the **destination interface** parameter with the appropriate argument to specify the interface to monitor. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

You can configure remote port mirroring by specifying the **remote vlan** keywords and an RSPAN VLAN ID. At the source switch, you must specify the destination as the RSPAN VLAN. At the destination switch, you must specify the source as the RSPAN VLAN. You cannot configure the source and destination as remote on the same switch.

Note: If an interface is a member of both a VLAN and a LAG, you cannot assign the VLAN as a destination VLAN for a monitor session. However, if an interface is a member of a VLAN and you assign the VLAN as a destination VLAN for a monitor session, afterwards you can add the interface as a member to a LAG.

Note: On an intermediate switch, you must create an RSPAN VLAN, make sure that the ports that are connected to the source and destination switches are members of the RSPAN VLAN, and enable RSPAN VLAN egress tagging on the port that is connected to the destination switch.

If you specify an RSPAN VLAN ID, you must also specify the reflector port at the source switch. The reflector port, which must be a member of the RSPAN VLAN, forwards the mirrored traffic to the destination switch. You specify the reflector port by entering the **reflector-port** keyword and the appropriate argument.

Format	<code>monitor session <i>session-id</i> destination {interface {<i>unit/slot/port</i> lag <i>lag-group-id</i>} remote vlan <i>vlan-id</i> reflector-port {<i>unit/slot/port</i> lag <i>lag-group-id</i>}}</code>

Mode	Global Config

no monitor session destination

This command removes a destination interface for a port mirroring session that is identified by the *session-id* argument (an integer value).

Format	<code>no monitor session <i>session-id</i> destination {interface remote vlan}</code>

Mode	Global Config

monitor session filter

M4250

M4350

This command attaches an IP ACL or MAC ACL to a selected monitor session by entering the access list number and name.

This command configures a probe port and a monitored port for a monitor session (port monitoring). Attaching a filter is not supported for an ERSPAN mirror session.

Format	<code>monitor session <i>session-id</i> filter {ip access-group <i>acl-id</i> <i>ip-acl-name</i>} mac access-group <i>mac-acl-name</i>}</code>

Mode	Global Config

Parameter	Description
<i>session-id</i>	The monitor session (port monitoring), which can be from 1 to 4.
<i>acl-id</i>	The IP ACL number.

Parameter	Description
<i>ip-acl-name</i>	The IP ACL name.
<i>mac-acl-name</i>	The MAC ACL name.

no monitor session filter

This command removes the specified IP ACL or MAC ACL from the selected monitoring session.

Format	<code>no monitor session <i>session-id</i> filter {ip access-group mac access-group}</code>
Mode	Global Config

monitor session mode

M4250

M4350

This command enables a specified port mirroring session.

Format	<code>monitor session <i>session-id</i> mode</code>
Mode	Global Config

no monitor session mode

This command disables the specified port mirroring session.

Format	<code>no monitor session <i>session-id</i> mode</code>
Mode	Global Config

no monitor

M4250

M4350

This command removes all the source ports and destination port and restores the default value for the mirroring session mode for all the configured sessions.

With the optional **session** keyword and *session-id* argument, this command removes the specified monitor session (port monitoring) designation from the source probe port, the destination monitored port, and all VLANs. When the port is removed from the VLAN, you must manually add the port to any desired VLANs.

Note: This is a stand-alone no command. This command does not have a normal form.

Format	<code>no monitor [session <i>session-id</i>]</code>

Mode	Global Config

show monitor session

M4250

M4350

This command displays the port monitoring information for a specific or all mirroring sessions.

The *session-id* parameter is an integer value used to identify the session. In the current version of the software, the *session-id* parameter is a number from 1 to 4.

Format	<code>show monitor session {<i>session-id</i> all}</code>

Mode	Privileged EXEC

Term	Definition
Session ID	An integer value used to identify the session. Its value can be anything between 1 and the maximum number of mirroring sessions allowed on the platform.
Monitor Session Mode	Indicates whether the Port Mirroring feature is enabled or disabled for the session identified with <i>session-id</i> . The possible values are Enabled and Disabled.
Probe Port	Probe port (destination port) for the session identified with <i>session-id</i> . If probe port is not set then this field is blank.
Source Port	The port, which is configured as mirrored port (source port) for the session identified with <i>session-id</i> . If no source port is configured for the session then this field is blank.
Type	Direction in which source port configured for port mirroring. Types are tx for transmitted packets and rx for receiving packets.
Src VLAN	All member ports of this VLAN are mirrored. If the source VLAN is not configured, this field is blank.
Ref. Port	This port carries all the mirrored traffic at the source switch.
Src Remote VLAN	The source VLAN is configured at the destination switch. If the remote VLAN is not configured, this field is blank.
Dst Remote VLAN	The destination VLAN is configured at the source switch. If the remote VLAN is not configured, this field is blank.
IP ACL	The IP access-list id or name attached to the port mirroring session.
MAC ACL	The MAC access-list name attached to the port mirroring session.

show vlan remote-span

M4250

M4350

This command displays the configured RSPAN VLAN.

Format	show vlan remote-span
Mode	Privileged Exec Mode

Command example:

```
(NETGEAR Switch)# show vlan remote-span
```

```
Remote SPAN VLAN
```

```
-----
100
```

ERSPAN Source Switch Configuration Commands

The Encapsulated Remote Port Analyzer (ERSPAN) feature allows port-mirroring collection points to be located anywhere across a routed network. This is achieved by encapsulating L2 mirrored packets using generic routing encapsulation (GRE) with IP delivery. After a packet is encapsulated, it can be forwarded throughout the L3-routed network.

ERSPAN uses a GRE tunnel to carry traffic between switches. ERSPAN consists of an ERSPAN source session, an ERSPAN destination session, and routable ERSPAN GRE-encapsulated traffic. All participating switches must be connected at Layer 3, and the network path must support the size of the ERSPAN traffic for the egress mirroring session.

To configure the source ERSPAN session, specify the following parameters at the source switch:

- Source ports (that is, the traffic on the source port is mirrored)
- ERSPAN destination IPv4 address
- ERSPAN origin IPv4 address
- ERSPAN session ID
- Egress (Tx) or ingress (Rx) traffic flow

monitor session type erspan-source

M4250**M4350**

This command specifies an ERSPAN source session ID, and the CLI enters ERSPAN Source Session Config mode. The *session-id* can be from 1 to 4.

Format	<code>monitor session <i>session-id</i> type erspan-source</code>
Mode	Global Config

no monitor session type erspan-source

This command removes an ERSPAN source session ID. The *session-id* can be from 1 to 4.

Format	<code>no monitor session <i>session-id</i> type erspan-source</code>
Mode	Global Config

source interface (ERSPAN Source Session Config)

M4250**M4350**

This command adds a source interface for an ERSPAN mirroring session. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Use the **source interface** {*unit/slot/port* | *cpu* | *lag lag-group-id* | *vlan vlan-id*} parameters to specify the interface to monitor.

Note: If an interface is a member of both a VLAN and a LAG, you cannot assign the VLAN as a source VLAN for a monitor session. However, if an interface is a member of a VLAN and you assign the VLAN as a source VLAN for a monitor session, afterwards you can add the interface as a member to a LAG.

Use **rx** to monitor only ingress packets or use **tx** to monitor only egress packets. If you do not specify an **rx** or **tx** option, the destination port monitors both ingress and egress packets.

Format	source {interface {unit/slot/port cpu lag lag-group-id} vlan vlan-id} [rx tx]

Mode	ERSPAN Source Session Config mode

no source interface (ERSPAN Source Session Config)

This command removes a source interface for an ERSPAN mirroring session.

Format	no source {interface {unit/slot/port cpu lag lag-group-id} vlan}

Mode	ERSPAN Source Session Config mode

destination (ERSPAN Source Session Config)

M4250

M4350

From the ERSPAN Source Session Config mode, this command lets the CLI enters ERSPAN Source Session Destination Config mode.

From this mode, you can specify the ERSPAN monitoring ID, IP settings, and origin settings for the ERSPAN destination.

Format	destination

Mode	ERSPAN Source Session Config

no destination (ERSPAN Source Session Config)

This command removes an ERSPAN source session destination configuration.

Format	no destination

Mode	ERSPAN Source Session Config

ip address (ERSPAN Source Session Destination Config)

M4250**M4350**

This command adds the destination IP address to an ERSPAN session. The IP address is the address of the monitoring station on which the GRE traffic is recorded or decoded.

Format	<code>ip address ip-address</code>
Mode	ERSPAN Source Session Destination Config

no ip address (ERSPAN Source Session Destination Config)

This command removes the destination IP address from an ERSPAN session.

Format	<code>no ip address</code>
Mode	ERSPAN Source Session Destination Config

erspan-id (ERSPAN Source Session Destination Config)

M4250**M4350**

This command adds the flow ID number that is used by the source and destination sessions to identify the ERSPAN traffic. The ID number is from 1 to 1023.

Format	<code>erspan-id erspan-id</code>
Mode	ERSPAN Source Session Destination Config

no erspan-id (ERSPAN Source Session Destination Config)

This command removes the flow ID number that is used by the source and destination sessions to identify the ERSPAN traffic.

Format	<code>no erspan-id</code>
Mode	ERSPAN Source Session Destination Config

origin ip address (ERSPAN Source Session Destination Config)

M4250**M4350**

This command adds the IP address that is used as the source of the ERSPAN traffic.

Format	<code>origin ip-address ip-address</code>

Mode	ERSPAN Source Session Destination Config

no origin ip address (ERSPAN Source Session Destination Config)

This command removes the IP address that is used as the source of the ERSPAN traffic.

Format	<code>no origin ip-address</code>

Mode	ERSPAN Source Session Destination Config

ip ttl (ERSPAN Source Session Destination Config)

M4250**M4350**

This command configures the IP time-to-live (TTL) value for the packets in the ERSPAN traffic. The range for the *ttl-value* argument is from 1 to 255.

Default	64

Format	<code>ip ttl ttl-value</code>

Mode	ERSPAN Source Session Destination Config

no ip ttl (ERSPAN Source Session Destination Config)

This command removes the TTL value for the packets in the ERSPAN traffic.

Format	<code>no ip ttl</code>

Mode	ERSPAN Source Session Destination Config

ip dscp (ERSPAN Source Session Destination Config)

M4250**M4350**

This command configures the IP DSCP value for the packets in the ERSPAN traffic. The range for the *dscp-value* argument is from 0 to 63.

Format	<code>ip dscp dscp-value</code>
Mode	ERSPAN Source Session Destination Config

no ip dscp (ERSPAN Source Session Destination Config)

This command removes the IP DSCP value for the packets in the ERSPAN traffic.

Format	<code>no ip dscp</code>
Mode	ERSPAN Source Session Destination Config

ip prec (ERSPAN Source Session Destination Config)

M4250**M4350**

This command configures the IP precedence value for the packets in the ERSPAN traffic. The range for the *precedence-value* argument is from 0 to 7.

Default	0
Format	<code>ip prec precedence-value</code>
Mode	ERSPAN Source Session Destination Config

no ip prec (ERSPAN Source Session Destination Config)

This command removes the IP DSCP value for the packets in the ERSPAN traffic.

Format	<code>no ip prec</code>
Mode	ERSPAN Source Session Destination Config

Static MAC Filtering Commands

The commands in this section describe how to configure static MAC filtering. Static MAC filtering allows you to configure destination ports for a static multicast MAC filter irrespective of the platform.

macfilter

M4250

M4350

This command adds a static MAC filter entry for the MAC address *macaddr* on the VLAN *vlanid*. A packet with a specific destination MAC address in a specific VLAN is admitted only if the ingress port is defined in the set of source ports, otherwise the packet is dropped.

On the egress side, a packet that was admitted is sent through all ports that are defined in the set of destination ports.

The value of the *macaddr* parameter is a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The restricted MAC Addresses are: 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, and FF:FF:FF:FF:FF:FF. The *vlanid* parameter must identify a valid VLAN.

The number of static mac filters supported on the system is different for MAC filters where source ports are configured and MAC filters where destination ports are configured.

- For unicast MAC address filters and multicast MAC address filters with source port lists, the maximum number of static MAC filters supported is 20.
- For multicast MAC address filters with destination ports configured, the maximum number of static filters supported is 256.

For example, you can configure the following combinations:

- Unicast MAC and source port (max = 20)
- Multicast MAC and source port (max = 20)
- Multicast MAC and destination port (only) (max = 256)
- Multicast MAC and source ports and destination ports (max = 20)

Format	<code>macfilter macaddr vlanid</code>
Mode	Global Config

no macfilter

M4250

M4350

This command removes all filtering restrictions and the static MAC filter entry for the MAC address *macaddr* on the VLAN *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The *vlanid* parameter must identify a valid VLAN.

Format	<code>no macfilter macaddr vlanid</code>
Mode	Global Config

macfilter adddest

M4250

M4350

Use this command to add the interface or range of interfaces to the destination filter set for the MAC filter with the specified *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Note: Configuring a destination port list is only valid for multicast MAC addresses.

Format	<code>macfilter adddest macaddr vlanid</code>
Mode	Interface Config

no macfilter adddest

This command removes a port from the destination filter set for the MAC filter with the specified *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format	<code>no macfilter adddest macaddr vlanid</code>
Mode	Interface Config

macfilter adddest all

M4250**M4350**

This command adds all interfaces to the destination filter set for the MAC filter with the specified *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Note: Configuring a destination port list is only valid for multicast MAC addresses.

Format	<code>macfilter adddest all <i>macaddr</i> <i>vlanid</i></code>

Mode	Global Config

no macfilter adddest all

This command removes all ports from the destination filter set for the MAC filter with the specified *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format	<code>no macfilter adddest all <i>macaddr</i> <i>vlanid</i></code>

Mode	Global Config

macfilter addsrc

M4250**M4350**

This command adds the interface or range of interfaces to the source filter set for the MAC filter with the specified *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format	<code>macfilter addsrc <i>macaddr</i> <i>vlanid</i></code>

Mode	Interface Config

no macfilter addsrc

This command removes a port from the source filter set for the MAC filter with the specified *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format	<code>no macfilter addsrc <i>macaddr</i> <i>vlanid</i></code>

Mode	Interface Config

macfilter addsrc all

M4250

M4350

This command adds all interfaces to the source filter set for the MAC filter with the MAC filter with the specified *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format	<code>macfilter addsrc all <i>macaddr</i> <i>vlanid</i></code>

Mode	Global Config

no macfilter addsrc all

This command removes all interfaces to the source filter set for the MAC filter with the specified *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format	<code>no macfilter addsrc all <i>macaddr</i> <i>vlanid</i></code>

Mode	Global Config

show mac-address-table static

M4250

M4350

This command displays the static MAC filtering information for all static MAC filters. If you specify **all**, all the static MAC filters in the system are displayed. If you supply a value for *macaddr*, you must also enter a value for **vlanid**, and the system displays static MAC filter information only for that MAC address and VLAN.

Format	<code>show mac-address-table static {<i>macaddr</i> <i>vlanid</i> all}</code>

Mode	Privileged EXEC

Term	Definition
MAC Address	The MAC address of the static MAC filter entry.

Term	Definition
VLAN ID	The VLAN ID of the static MAC filter entry.
Source Ports	The source port of the static MAC filter entry.

Note: Only multicast address filters can have destination port lists.

show mac-address-table staticfiltering

M4250

M4350

This command displays the Static Filtering entries in the Multicast Forwarding Database (MFDB) table.

Format	<code>show mac-address-table staticfiltering</code>
Mode	Privileged EXEC

Term	Definition
VLAN ID	The VLAN in which the MAC Address is learned.
MAC Address	A unicast MAC address for which the switch has forwarding and or filtering information. As the data is gleaned from the MFDB, the address will be a multicast address. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	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.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

DHCP L2 Relay Agent Commands

You can enable the switch to operate as a DHCP Layer 2 relay agent to relay DHCP requests from clients to a Layer 3 relay agent or server. The Circuit ID and Remote ID can be added to DHCP requests relayed from clients to a DHCP server. This information is included in DHCP Option 82, as specified in sections 3.1 and 3.2 of RFC3046.

dhcp l2relay

M4250**M4350**

This command enables the DHCP Layer 2 Relay agent for an interface a range of interfaces in, or all interfaces. The subsequent commands mentioned in this section can only be used when the DHCP L2 relay is enabled.

Format	<code>dhcp l2relay</code>
Mode	Global Config Interface Config

no dhcp l2relay

This command disables DHCP Layer 2 relay agent for an interface or range of interfaces.

Format	<code>no dhcp l2relay</code>
Mode	Global Config Interface Config

dhcp l2relay circuit-id vlan

M4250**M4350**

This command sets the DHCP Option-82 Circuit ID for a VLAN. If enabled, the interface number is added as the Circuit ID in DHCP option 82.

Format	<code>dhcp l2relay circuit-id vlan <i>vlan-list</i></code>
Mode	Global Config

Parameter	Description
<code>vlan-list</code>	The VLAN ID. The range is 1–4093. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no dhcp l2relay circuit-id vlan

This parameter removes the DHCP Option-82 Circuit ID for a VLAN.

Format	<code>no dhcp l2relay circuit-id vlan <i>vlan-list</i></code>
Mode	Global Config

dhcp l2relay remote-id

M4250

M4350

This command sets the DHCP Option-82 Remote ID for a VLAN. The *remote-id* is a character string.

Format	dhcp l2relay remote-id <i>remote-id</i> vlan <i>vlan-list</i>
Mode	Global Config
Parameter	Description
vlan-list	The VLAN ID. The range is 1–4093. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no dhcp l2relay remote-id vlan

This parameter clears the DHCP Option-82 Remote ID for a VLAN.

Format	no dhcp l2relay <i>remote-id</i> vlan <i>vlan-list</i>
Mode	Global Config

dhcp l2relay vlan

M4250

M4350

Use this command to enable the DHCP L2 Relay agent for a set of VLANs. All DHCP packets which arrive on interfaces in the configured VLAN are subject to L2 Relay processing.

Default	Disabled
Format	dhcp l2relay vlan <i>vlan-list</i>
Mode	Global Config
Parameter	Description
vlan-list	The VLAN ID. The range is 1–4093. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no dhcp l2relay vlan

Use this command to disable the DHCP L2 Relay agent for a set of VLANs.

Format	no dhcp l2relay vlan <i>vlan-list</i>
Mode	Global Config

dhcp l2relay circuit-id

M4250

M4350

This command sets the DHCP Option-82 Circuit ID for an interface.

Format	<code>dhcp l2relay circuit-id <i>circuitid-string</i></code>
Mode	Interface Config
Parameter	Description
circuitid-string	The circuit ID suboption string of up to 64 characters.

no dhcp l2relay circuit-id

This removes the DHCP Option-82 Circuit ID for an interface.

Format	<code>no dhcp l2relay circuit-id</code>
Mode	Interface Config

dhcp l2relay trust

M4250

M4350

Use this command to configure an interface or range of interfaces as trusted for Option-82 reception.

The **no-option-82 update** keywords enable the addition of Option-82 to packets received on the trusted interface without Option-82.

Default	Untrusted
Format	<code>dhcp l2relay trust [no-option-82 update]</code>
Mode	Interface Config

no dhcp l2relay trust

Use this command to configure an interface to the default untrusted for Option-82 reception.

Format	<code>no dhcp l2relay trust [no-option-82 update]</code>
Mode	Interface Config

show dhcp l2relay all

M4250

M4350

This command displays the summary of DHCP L2 Relay configuration.

Format	show dhcp l2relay all

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show dhcp l2relay all
```

DHCP L2 Relay is Enabled.

Interface	L2RelayMode	TrustMode
0/2	Enabled	untrusted
0/4	Disabled	trusted

VLAN Id	L2 Relay	CircuitId	RemoteId
3	Disabled	Enabled	--NULL--
5	Enabled	Enabled	--NULL--
6	Enabled	Enabled	NETGEAR
7	Enabled	Disabled	--NULL--
8	Enabled	Disabled	--NULL--
9	Enabled	Disabled	--NULL--
10	Enabled	Disabled	--NULL--

show dhcp l2relay circuit-id vlan

M4250

M4350

This command displays the DHCP circuit ID VLAN configuration.

Format	show dhcp l2relay circuit-id vlan <i>vlan-list</i>

Mode	Privileged EXEC

Parameter	Description
vlan-list	Enter VLAN IDs in the range 1–4093. Use a dash (–) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.

show dhcp l2relay interface

M4250**M4350**

This command displays DHCP L2 relay configuration that is specific to interfaces.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show dhcp l2relay interface {all <i>unit/slot/port</i> }
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show dhcp l2relay interface all
```

```
DHCP L2 Relay is Enabled.
```

Interface	L2RelayMode	TrustMode
-----	-----	-----
0/2	Enabled	untrusted
0/4	Disabled	trusted

show dhcp l2relay remote-id vlan

M4250**M4350**

This command displays the DHCP remote ID VLAN configuration.

Format	show dhcp l2relay remote-id vlan <i>vlan-list</i>
Mode	Privileged EXEC

Parameter	Description
vlan-list	Enter VLAN IDs in the range 1–4093. Use a dash (–) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.

show dhcp l2relay stats interface

M4250**M4350**

This command displays statistics specific to DHCP L2 Relay configured interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	show dhcp l2relay stats interface {all <i>unit/slot/port</i> }

Mode	Privileged EXEC

Command example:

```
((NETGEAR Switch)) #show dhcp l2relay stats interface all
```

```
DHCP L2 Relay is Enabled.
```

Interface	UntrustedServer MsgsWithOpt82	UntrustedClient MsgsWithOpt82	TrustedServer MsgsWithoutOpt82	TrustedClient MsgsWithoutOpt82
-----	-----	-----	-----	-----
0/1	0	0	0	0
0/2	0	0	3	7
0/3	0	0	0	0
0/4	0	12	0	0
0/5	0	0	0	0
0/6	3	0	0	0
0/7	0	0	0	0
0/8	0	0	0	0
0/9	0	0	0	0

show dhcp l2relay agent-option vlan

M4250**M4350**

This command displays the DHCP L2 Relay Option-82 configuration specific to VLAN.

Format	show dhcp l2relay agent-option vlan <i>vlan-range</i>

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show dhcp l2relay agent-option vlan 5-10
```

```
DHCP L2 Relay is Enabled.
```

VLAN Id	L2 Relay	CircuitId	RemoteId
5	Enabled	Enabled	--NULL--
6	Enabled	Enabled	NETGEAR
7	Enabled	Disabled	--NULL--
8	Enabled	Disabled	--NULL--
9	Enabled	Disabled	--NULL--
10	Enabled	Disabled	--NULL--

```
show dhcp l2relay vlan
```

M4250

M4350

This command displays the DHCP VLAN configuration.

Format	<code>show dhcp l2relay vlan <i>vlan-list</i></code>

Mode	Privileged EXEC

Parameter	Description
vlan-list	Enter VLAN IDs in the range 1–4093. Use a dash (–) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.

```
clear dhcp l2relay statistics interface
```

M4250

M4350

Use this command to reset the DHCP L2 relay counters to zero. Specify the port with the counters to clear, or use the **all** keyword to clear the counters on all ports. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>clear dhcp l2relay statistics interface {<i>unit/slot/port</i> all}</code>

Mode	Privileged EXEC

DHCP Client Commands

The switch can include vendor and configuration information in DHCP client requests relayed to a DHCP server. This information is included in DHCP Option 60, Vendor Class Identifier. The information is a string of 128 octets.

`dhcp client vendor-id-option`

M4250

M4350

This command enables the inclusion of DHCP Option-60, Vendor Class Identifier. This information is included in the requests transmitted to the DHCP server by the DHCP client operating in the switch.

Format	<code>dhcp client vendor-id-option</code>
Mode	Global Config

`no dhcp client vendor-id-option`

This command disables the inclusion of DHCP Option-60.

Format	<code>no dhcp client vendor-id-option</code>
Mode	Global Config

`dhcp client vendor-id-option-string`

M4250

M4350

This command sets the DHCP Vendor Option-60 string. This information is included in the requests transmitted to the DHCP server by the DHCP client operating on the switch.

Format	<code>dhcp client vendor-id-option-string <i>string</i></code>
Mode	Global Config

`no dhcp client vendor-id-option-string`

This command disables the inclusion of the DHCP Option-60 string.

Format	<code>no dhcp client vendor-id-option-string</code>
Mode	Global Config

show dhcp client vendor-id-option

M4250

M4350

This command displays the configured administration mode of the vendor-id-option and the vendor-id string to be included in Option-43 in DHCP requests.

Format	show dhcp client vendor-id-option

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show dhcp client vendor-id-option
```

```
DHCP Client Vendor Identifier Option..... Enabled
DHCP Client Vendor Identifier Option String.... NetgearClient
```

DHCP Snooping Configuration Commands

This section describes commands you use to configure DHCP Snooping.

ip dhcp snooping

M4250

M4350

Use this command to enable DHCP Snooping globally.

Default	Disabled

Format	ip dhcp snooping

Mode	Global Config

no ip dhcp snooping

Use this command to disable DHCP Snooping globally.

Format	no ip dhcp snooping

Mode	Global Config

ip dhcp snooping vlan

M4250

M4350

Use this command to enable DHCP Snooping on a VLAN or a list of comma-separated VLAN ranges.

Default	Disabled
Format	<code>ip dhcp snooping vlan <i>vlan-list</i></code>
Mode	Global Config

no ip dhcp snooping vlan

Use this command to disable DHCP Snooping on VLANs.

Format	<code>no ip dhcp snooping vlan <i>vlan-list</i></code>
Mode	Global Config

ip dhcp snooping verify mac-address

M4250

M4350

Use this command to enable verification of the source MAC address with the client hardware address in the received DHCP message.

Default	Enabled
Format	<code>ip dhcp snooping verify mac-address</code>
Mode	Global Config

no ip dhcp snooping verify mac-address

Use this command to disable verification of the source MAC address with the client hardware address.

Format	<code>no ip dhcp snooping verify mac-address</code>
Mode	Global Config

ip dhcp snooping database

M4250**M4350**

Use this command to configure the persistent location of the DHCP Snooping database. This can be local or a remote file.

Default	Local
Format	<code>ip dhcp snooping database {local tftp://hostIP/filename}</code>
Mode	Global Config

ip dhcp snooping database write-delay (DHCP)

M4250**M4350**

Use this command to configure the interval in seconds at which the DHCP Snooping database persists. The interval value ranges from 15 to 86400 seconds.

Default	300 seconds
Format	<code>ip dhcp snooping database write-delay seconds</code>
Mode	Global Config

no ip dhcp snooping database write-delay

Use this command to set the write delay value to the default value.

Format	<code>no ip dhcp snooping database write-delay</code>
Mode	Global Config

ip dhcp snooping binding

M4250**M4350**

Use this command to configure a static DHCP Snooping binding. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>ip dhcp snooping binding <i>mac-address</i> vlan <i>vlan-id</i> <i>ipaddress</i> interface {<i>unit/slot/port</i> lag <i>lag-group-id</i>} [<i>expiry lease-in-seconds</i>]</code>

Mode	Global Config

`no ip dhcp snooping binding`

Use this command to remove a DHCP static entry from the DHCP Snooping database.

Format	<code>no ip dhcp snooping binding <i>mac-address</i></code>

Mode	Global Config

`ip verify binding`

M4250

M4350

Use this command to configure static IP source guard (IPSG) entries. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>ip verify binding <i>mac-address</i> vlan <i>vlan-id</i> <i>ipaddress</i> interface {<i>unit/slot/port</i> lag <i>lag-group-id</i>}</code>

Mode	Global Config

`no ip verify binding`

Use this command to remove the IPSG static entry from the IPSG database.

Format	<code>no ip verify binding <i>mac-address</i> vlan <i>vlan-id</i> <i>ipaddress</i> interface {<i>unit/slot/port</i> lag <i>lag-group-id</i>}</code>

Mode	Global Config

`ip dhcp snooping limit`

M4250

M4350

Use this command to control the rate at which the DHCP Snooping messages come on an interface or range of interfaces. By default, rate limiting is disabled. When enabled, the rate can range from 0 to 300 packets per second (pps). The burst level range is 1 to 15 seconds. You can also use the **none** keyword to set no limit.

Default	Disabled (no limit)
Format	<code>ip dhcp snooping limit {rate <i>pps</i> [burst interval <i>seconds</i>] none}</code>
Mode	Interface Config

no ip dhcp snooping limit

Use this command to set the rate at which the DHCP Snooping messages come, and the burst level, to the defaults.

Format	<code>no ip dhcp snooping limit</code>
Mode	Interface Config

ip dhcp snooping log-invalid

M4250

M4350

Use this command to control the logging DHCP messages filtration by the DHCP Snooping application. This command can be used to configure a single interface or a range of interfaces.

Default	Disabled
Format	<code>ip dhcp snooping log-invalid</code>
Mode	Interface Config

no ip dhcp snooping log-invalid

Use this command to disable the logging DHCP messages filtration by the DHCP Snooping application.

Format	<code>no ip dhcp snooping log-invalid</code>
Mode	Interface Config

ip dhcp snooping trust

M4250

M4350

Use this command to configure an interface or range of interfaces as trusted.

Default	Disabled
Format	ip dhcp snooping trust
Mode	Interface Config

no ip dhcp snooping trust

Use this command to configure the port as untrusted.

Format	no ip dhcp snooping trust
Mode	Interface Config

ip verify source

M4250

M4350

Use this command to configure the IPSG source ID attribute to filter the data traffic in the hardware. Source ID is the combination of IP address and MAC address. Normal command allows data traffic filtration based on the IP address. With the **port-security** option, the data traffic will be filtered based on the IP and MAC addresses.

This command can be used to configure a single interface or a range of interfaces.

Default	The source ID is the IP address
Format	ip verify source [port-security]
Mode	Interface Config

no ip verify source

Use this command to disable the IPSG configuration in the hardware. You cannot disable port-security alone if it is configured.

Format	no ip verify source
Mode	Interface Config

show ip dhcp snooping

M4250**M4350**

Use this command to display the DHCP Snooping global configurations and per port configurations.

Format	show ip dhcp snooping
Mode	Privileged EXEC User EXEC
Term	Definition
Interface	The interface for which data is displayed.
Trusted	If it is enabled, DHCP snooping considers the port as trusted. The factory default is disabled.
Log Invalid Pkts	If it is enabled, DHCP snooping application logs invalid packets on the specified interface.

Command example:

```
(NETGEAR Switch) #show ip dhcp snooping
```

```
DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
11 - 30, 40
```

Interface	Trusted	Log Invalid Pkts
-----	-----	-----
0/1	Yes	No
0/2	No	Yes
0/3	No	Yes
0/4	No	No
0/6	No	No

show ip dhcp snooping binding

M4250**M4350**

Use this command to display the DHCP Snooping binding entries.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

To restrict the output, use the following options:

- **static**. Restrict the output based on static entries.
- **dynamic**. Restrict the output based on DHCP snooping.
- **interface** *unit/slot/port*. Restrict the output based on a specific interface.
- *vlan-id*. Restrict the output based on a VLAN.

Format	<code>show ip dhcp snooping binding [static dynamic] [interface unit/slot/port] [vlan-id]</code>
Mode	Privileged EXEC User EXEC

Term	Definition
MAC Address	Displays the MAC address for the binding that was added. The MAC address is the key to the binding database.
IP Address	Displays the valid IP address for the binding rule.
VLAN	The VLAN for the binding rule.
Interface	The interface to add a binding into the DHCP snooping interface.
Type	Binding type; statically configured from the CLI or dynamically learned.
Lease (sec)	The remaining lease time for the entry.

Command example:

```
(NETGEAR Switch) #show ip dhcp snooping binding
```

Total number of bindings: 2

MAC Address	IP Address	VLAN	Interface	Type	Lease time (Secs)
00:02:B3:06:60:80	210.1.1.3	10	0/1		86400
00:0F:FE:00:13:04	210.1.1.4	10	0/1		86400

show ip dhcp snooping database

M4250

M4350

Use this command to display the DHCP Snooping configuration related to the database persistency.

Format	<code>show ip dhcp snooping database</code>
Mode	Privileged EXEC User EXEC

Term	Definition
Agent URL	Bindings database agent URL.
Write Delay	The maximum write time to write the database into local or remote.

Command example:

```
(NETGEAR Switch) #show ip dhcp snooping database
agent url: /10.131.13.79:/sail.txt
write-delay: 5000
```

show ip dhcp snooping interfaces

M4250**M4350**

Use this command to show the DHCP Snooping status of the interfaces or of a specific interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show ip dhcp snooping interfaces [<i>unit/slot/port</i>]
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show ip dhcp snooping interfaces
```

Interface	Trust State	Rate Limit (pps)	Burst Interval (seconds)
1/0/1	No	15	1
1/0/2	No	15	1
1/0/3	No	15	1

Command example:

```
(NETGEAR Switch) #show ip dhcp snooping interfaces ethernet 1/0/15
```

Interface	Trust State	Rate Limit (pps)	Burst Interval (seconds)
1/0/15	Yes	15	1

show ip dhcp snooping statistics

M4250

M4350

Use this command to list statistics for DHCP Snooping security violations on untrusted ports.

Format	show ip dhcp snooping statistics
Mode	Privileged EXEC User EXEC
Term	Definition
Interface	The IP address of the interface in unit/slot/port format.
MAC Verify Failures	Represents the number of DHCP messages that were filtered on an untrusted interface because of source MAC address and client HW address mismatch.
Client Ifc Mismatch	Represents the number of DHCP release and Deny messages received on the different ports than learned previously.
DHCP Server Msgs Rec'd	Represents the number of DHCP server messages received on Untrusted ports.

Command example:

```
(NETGEAR Switch) #show ip dhcp snooping statistics
```

Interface	MAC Verify Failures	Client Ifc Mismatch	DHCP Server Msgs Rec'd
-----	-----	-----	-----
1/0/2	0	0	0
1/0/3	0	0	0
1/0/4	0	0	0
1/0/5	0	0	0
1/0/6	0	0	0
1/0/7	0	0	0
1/0/8	0	0	0
1/0/9	0	0	0
1/0/10	0	0	0
1/0/11	0	0	0
1/0/12	0	0	0
1/0/13	0	0	0
1/0/14	0	0	0
1/0/15	0	0	0
1/0/16	0	0	0
1/0/17	0	0	0
1/0/18	0	0	0
1/0/19	0	0	0
1/0/20	0	0	0

clear ip dhcp snooping binding

M4250**M4350**

Use this command to clear all DHCP Snooping bindings on all interfaces or on a specific interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>clear ip dhcp snooping binding [interface <i>unit/slot/port</i>]</code>
Mode	Privileged EXEC User EXEC

clear ip dhcp snooping statistics

M4250**M4350**

Use this command to clear all DHCP Snooping statistics.

Format	<code>clear ip dhcp snooping statistics</code>
Mode	Privileged EXEC User EXEC

show ip verify

M4250**M4350**

Use this command to display the IPSG filter type for all interfaces or for a specific interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show ip verify [interface <i>unit/slot/port</i>]</code>
Mode	Privileged EXEC User EXEC

Term	Definition
Interface	The interface.
Filter Type	One of two values: ip-mac: User has configured MAC address filtering on this interface. ip: Only IP address filtering on this interface.

show ip verify source

M4250

M4350

Use this command to display the IPSG configurations on all interfaces or for a specific interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show ip verify source [interface <i>unit/slot/port</i>]
Mode	Privileged EXEC User EXEC

Term	Definition
Interface	The Interface.
Filter Type	One of two values: ip-mac: User has configured MAC address filtering on this interface. ip: Only IP address filtering on this interface.
IP Address	IP address of the interface
MAC Address	If MAC address filtering is not configured on the interface, the MAC Address field is empty. If port security is disabled on the interface, then the MAC Address field displays "permit-all."
VLAN	The VLAN for the binding rule.

Command example:

```
(NETGEAR Switch) #show ip verify source
```

Interface	Filter Type	IP Address	MAC Address	Vlan
-----	-----	-----	-----	-----
0/1	ip-mac	210.1.1.3	00:02:B3:06:60:80	10
0/1	ip-mac	210.1.1.4	00:0F:FE:00:13:04	10

show ip source binding

M4250

M4350

Use this command to display the IPSG bindings. As an option, you can display the DHCP snooping bindings or static bindings, the bindings for a specific interface, or the bindings for a VLAN. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show ip source binding [dhcp-snooping static] [interface <i>unit/slot/port</i> vlan <i>vlan-id</i>]
Mode	Privileged EXEC User EXEC
Term	Definition
MAC Address	The MAC address for the entry that is added.
IP Address	The IP address of the entry that is added.
Type	Entry type; statically configured from CLI or dynamically learned from DHCP Snooping.
VLAN	VLAN for the entry.
Interface	IP address of the interface in <i>unit/slot/port</i> format.

Command example:

```
(NETGEAR Switch) #show ip source binding
```

MAC Address	IP Address	Type	Vlan	Interface
-----	-----	-----	-----	-----
00:00:00:00:00:08	1.2.3.4	dhcp-snooping	2	1/0/1
00:00:00:00:00:09	1.2.3.4	dhcp-snooping	3	1/0/1
00:00:00:00:00:0A	1.2.3.4	dhcp-snooping	4	1/0/1

Dynamic ARP Inspection Commands

Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. DAI prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address.

DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a binding database of valid MAC addresses, IP addresses, VLANs, and interfaces.

When DAI is enabled, the switch drops ARP packets whose sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. You can optionally configure additional ARP packet validation.

`ip arp inspection vlan`

M4250

M4350

Use this command to enable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Default	Disabled
Format	<code>ip arp inspection vlan <i>vlan-list</i></code>
Mode	Global Config

`no ip arp inspection vlan`

Use this command to disable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Format	<code>no ip arp inspection vlan <i>vlan-list</i></code>
Mode	Global Config

`ip arp inspection validate`

M4250

M4350

Use this command to enable additional validation checks such as source MAC address (src-mac) validation, destination MAC address (dst-mac) validation, IP address validation, and interface validation on the received ARP packets. You can also enable a combination of such validations.

Each instance of the command overrides the configuration of the previous command. For example, if a command enables source-mac and destination-mac validations, and a second command enables IP validation only, the source-mac and destination-mac validations are disabled as a result of the second command.

Default	Disabled
Format	<code>ip arp inspection validate {[src-mac [dst-mac] [ip]] [dst-mac [ip]] ip interface}</code>
Mode	Global Config

no ip arp inspection validate

Use this command to disable the additional validation checks on the received ARP packets.

Format	no ip arp inspection validate {[src-mac [dst-mac] [ip]] [dst-mac [ip]] ip interface}
Mode	Global Config

ip arp inspection vlan

M4250

M4350

Use this command to enable additional validation checks on the ARP packets that are received on a VLAN or a list of comma-separated VLAN ranges. As an option, you can enable logging of invalid ARP packets and set an interval from 0 to 86400 minutes.

Default	Enabled
Format	ip arp inspection vlan <i>vlan-list</i> [logging] [interval <i>minutes</i>]
Mode	Global Config

no ip arp inspection vlan

Use this command to disable additional validation checks on the ARP packets that are received on a VLAN or a list of comma-separated VLAN ranges, and disable logging of invalid ARP packets.

Format	no ip arp inspection vlan <i>vlan-list</i> [logging] [interval]
Mode	Global Config

ip arp inspection trust

M4250

M4350

Use this command to configure an interface or range of interfaces as trusted for Dynamic ARP Inspection.

Default	Disabled
Format	ip arp inspection trust
Mode	Interface Config

no ip arp inspection trust

Use this command to configure an interface as untrusted for Dynamic ARP Inspection.

Format	no ip arp inspection trust

Mode	Interface Config

ip arp inspection limit

M4250

M4350

Use this command to configure the rate limit and burst interval values for an interface or range of interfaces. Configuring **none** for the limit means the interface is not rate limited for Dynamic ARP Inspections. The maximum packets per second (pps) value shown in the range for the rate option might be more than the hardware-allowable limit. Therefore, we recommend that you take the switch performance into account before you configure the maximum pps rate. The pps rate range is from 0 to 300 pps. The burst interval is from 1 to 15 seconds.

Note: The user interface accepts a rate limit for a trusted interface, but the limit is not enforced unless the interface is configured to be untrusted.

Default	15 pps for rate and 1 second for burst-interval.

Format	ip arp inspection limit {rate pps [burst interval seconds] none}

Mode	Interface Config

no ip arp inspection limit

Use this command to set the rate limit and burst interval values for an interface to the default values of 15 pps and 1 second, respectively.

Format	no ip arp inspection limit

Mode	Interface Config

ip arp inspection filter

M4250**M4350**

Use this command to configure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges. If the static keyword is specified, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings.

Default	No ARP ACL is configured on a VLAN.
Format	<code>ip arp inspection filter <i>acl-name</i> vlan <i>vlan-list</i> [static]</code>
Mode	Global Config

no ip arp inspection filter

Use this command to unconfigure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges.

Format	<code>no ip arp inspection filter <i>acl-name</i> vlan <i>vlan-list</i> [static]</code>
Mode	Global Config

arp access-list

M4250**M4350**

Use this command to create an ARP ACL and let the CLI enter the ARP Access-list Config mode.

Format	<code>arp access-list <i>acl-name</i></code>
Mode	Global Config

no arp access-list

Use this command to delete a configured ARP ACL.

Format	<code>no arp access-list <i>acl-name</i></code>
Mode	Global Config

permit ip host mac host

M4250

M4350

Use this command to configure a rule that permits a sender's IP address and MAC address combination for ARP packet validation.

Format	permit ip {any host <i>ip-address</i> } mac {any host <i>mac-address</i> }

Mode	ARP Access-list Config

no permit ip host mac host

Use this command to delete a rule that permits a sender's IP address and MAC address combination.

Format	no permit ip {any host <i>ip-address</i> } mac {any host <i>mac-address</i> }

Mode	ARP Access-list Config

deny ip host mac host

M4250

M4350

Use this command to configure a rule that denies a sender's IP address and MAC address combination for ARP packet validation.

Format	deny ip {any host <i>ip-address</i> } mac {any host <i>mac-address</i> }

Mode	ARP Access-list Config

no deny ip host mac host

Use this command to delete a rule that denies a sender's IP address and MAC address combination.

Format	no deny ip {any host <i>ip-address</i> } mac {any host <i>mac-address</i> }

Mode	ARP Access-list Config

remark

M4250

M4350

Use this command to add a remark to the ARL ACL.

Format	<i>remark string</i>
Mode	ARP Access-list Config

no remark

Use this command to delete a remark from the ARL ACL.

Format	<i>no remark string</i>
Mode	ARP Access-list Config

show ip arp inspection

M4250

M4350

Use this command to display the Dynamic ARP Inspection global configuration and configuration on all the VLANs. With the optional **vlan** keyword and *vlan-list* argument (that is, comma separated VLAN ranges), the command displays the global configuration and configuration on all the VLANs in the VLAN list. For the *vlan-list* argument, you can enter a list of VLANs (for example, 12-18 or 12,14) to display the statistics on all DAI-enabled VLANs in the list, or enter a single VLAN to display the statistics for only that VLAN. The global configuration includes the source mac validation, destination mac validation and invalid IP validation information.

Format	<i>show ip arp inspection [vlan vlan-list]</i>
Mode	Privileged EXEC User EXEC

Term	Definition
Source MAC Validation	Displays whether Source MAC Validation of ARP frame is enabled or disabled.
Destination MAC Validation	Displays whether Destination MAC Validation is enabled or disabled.
IP Address Validation	Displays whether IP Address Validation is enabled or disabled.
VLAN	The VLAN ID for each displayed row.
Configuration	Displays whether DAI is enabled or disabled on the VLAN.

Term	Definition
Log Invalid	Displays whether logging of invalid ARP packets is enabled on the VLAN.
ACL Name	The ARP ACL Name, if configured on the VLAN.
Static Flag	If the ARP ACL is configured static on the VLAN.

Command example:

```
(NETGEAR Switch) #show ip arp inspection vlan 10-12
```

```
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
```

Vlan	Configuration	Log Invalid	ACL Name	Static flag
----	-----	-----	-----	-----
10	Enabled	Enabled	H2	Enabled
11	Disabled	Enabled		
12	Enabled	Disabled		

show ip arp inspection statistics

M4250**M4350**

Use this command to display the statistics of the ARP packets that are processed by Dynamic ARP Inspection (DAI). For the optional **vlan** keyword and *vlan-list* argument, you can enter a list of VLANs (for example, 12-18 or 12,14) to display the statistics on all DAI-enabled VLANs in the list, or enter a single VLAN to display the statistics for only that VLAN. If you do not include the **vlan** keyword and *vlan-list* argument, the command output displays a summary of the forwarded and dropped ARP packets.

Format show ip arp inspection statistics [vlan *vlan-list*]

Mode Privileged EXEC
 User EXEC

Term	Definition
VLAN	The VLAN ID for each displayed row.
Forwarded	The total number of valid ARP packets forwarded in this VLAN.
Dropped	The total number of not valid ARP packets dropped in this VLAN.
DHCP Drops	The number of packets dropped due to DHCP snooping binding database match failure.
ACL Drops	The number of packets dropped due to ARP ACL rule match failure.

Term	Definition
DHCP Permits	The number of packets permitted due to DHCP snooping binding database match.
ACL Permits	The number of packets permitted due to ARP ACL rule match.
Bad Src MAC	The number of packets dropped due to Source MAC validation failure.
Bad Dest MAC	The number of packets dropped due to Destination MAC validation failure.
Invalid IP	The number of packets dropped due to invalid IP checks.

Command example:

The output of the **show ip arp inspection statistics** command lists the summary of forwarded and dropped ARP packets on all DAI-enabled VLANs:

```
VLAN  Forwarded  Dropped
----  -
10      90      14
20      10      3
```

Command example:

```
(NETGEAR Switch) #show ip arp inspection statistics vlan vlan-list
```

```
VLAN      DHCP      ACL      DHCP      ACL      Bad Src      Bad Dest      Invalid
          Drops      Drops      Permits      Permits      MAC          MAC          IP
-----
10         11         1         65         25         1           1           0
20          1         0          8          2         0           1           1
```

clear ip arp inspection statistics

M4250

M4350

Use this command to reset the statistics for Dynamic ARP Inspection on all VLANs.

Default	none
Format	clear ip arp inspection statistics
Mode	Privileged EXEC

show ip arp inspection interfaces

M4250**M4350**

Use this command to display the Dynamic ARP Inspection configuration on all the DAI-enabled interfaces. An interface is said to be enabled for DAI if at least one VLAN, that the interface is a member of, is enabled for DAI. If you enter the optional interface argument, the command displays the values for that interface whether the interface is enabled for DAI or not. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show ip arp inspection interfaces [<i>unit/slot/port</i>]
Mode	Privileged EXEC User EXEC
Term	Definition
Interface	The interface ID for each displayed row.
Trust State	Whether the interface is trusted or untrusted for DAI.
Rate Limit	The configured rate limit value in packets per second.
Burst Interval	The configured burst interval value in seconds.

Command example:

```
(NETGEAR Switch) #show ip arp inspection interfaces
```

Interface	Trust State	Rate Limit (pps)	Burst Interval (seconds)
0/1	Untrusted	15	1
0/2	Untrusted	10	10

show arp access-list

M4250**M4350**

Use this command to display the configured ARP ACLs with the rules. Giving an ARP ACL name as the argument displays only the rules in that ARP ACL.

Format	show arp access-list [<i>acl-name</i>]
Mode	Privileged EXEC User EXEC

Command example:

```
(NETGEAR Switch) #show arp access-list
ARP access list H2
    permit ip host 1.1.1.1 mac host 00:01:02:03:04:05
    permit ip host 1.1.1.2 mac host 00:03:04:05:06:07
ARP access list H3
ARP access list H4
    permit ip host 2.1.1.2 mac host 00:03:04:05:06:08
```

ARP Guard Commands

The ARP Guard feature protects the switch CPU from DoS attacks with ARP messages. This feature provides the following:

- Rate limiting of incoming ARP packets on a per-host basis.
- Detecting and logging an ARP attack from a host, when a threshold is crossed.

arp-guard enable

M4250

M4350

Use this command to enable the ARP Guard feature globally.

Default	Disabled
Format	arp-guard enable
Mode	Global Config

no arp-guard enable

Use this command to disable the ARP Guard feature and clear all the operational entries in all ARP Guard tables.

Format	no arp-guard enable
Mode	Global Config

arp-guard rate-limit

M4250

M4350

Use this command to configure the rate limit for ARP packet processing at a rate measured in packets-per-second. You can configure the ARP packets rate limit independently on a per-port basis and on a per-host basis (hosts identified based on source IP address, VLAN

ID, and port and hosts identified based on the link-layer source MAC address, VLAN ID, and port).

Default	Although the range is the same for all ARP rate limiting types, the default values vary and are as follows: - Per-port rate limit: Default 15. - Per-host (SMAC) rate limit: Default 10. - Per-host (SIP) rate limit: Default 10.

Format	<code>arp-guard rate-limit {per-src-ip per-src-mac per-port} pps</code>

Mode	Global Config

Term	Definition
per-src-ip	Limits the rate of each source IP address.
per-src-mac	Limits the rate of each source MAC address.
per-port	Limits the rate of each port.
pps	The rate limit in packets-per-second, ranging from 0 to 300. A value of zero (0) means no limit, that is, the value is not tracked.

Command example:

```
(NETGEAR Switch) (Config)# arp-guard rate-limit per-src-ip 100
```

no arp-guard rate-limit

Use this command to reset the rate limit to the corresponding default value.

Format	<code>no arp-guard rate-limit {per-src-ip per-src-mac per-port}</code>

Mode	Global Config

arp-guard attack-threshold

M4250

M4350

Use this command to configure the attack threshold for ARP packets attack detection at a rate measured in packets-per-second. You can configure the ARP packets attack threshold independently on a per-port basis and on a per-host basis (hosts identified based on source IP address, VLAN ID, and port and hosts identified based on the link-layer source MAC address, VLAN ID, and port).

Default	Although the range is the same for all ARP rate limiting types, the default values vary and are as follows: • Per-port attack threshold default: 30. • Per-host (SMAC) attack threshold default: 20. • Per-host (SIP) attack threshold default: 20.
Format	<code>arp-guard attack-threshold {per-src-ip per-src-mac per-port} pps</code>
Mode	Global Config

Term	Definition
per-src-ip	Detects ARP attacks by hosts identified by source IP address.
per-src-mac	Detects ARP attacks by hosts identified by source MAC address.
per-port	Detects ARP attacks by port.
pps	The rate limit in packets-per-second, ranging from 0 to 300. A value of zero (0) means no limit, that is, the value is not tracked.

Command example:

```
(NETGEAR Switch) (Config)# arp-guard attack-threshold per-src-mac 100
```

`no arp-guard attack-threshold`

Use this command to reset the attack threshold to the corresponding default value. The attack threshold for a tracking type must always equal or exceed the corresponding rate limit on the port. An error occurs if configured otherwise. An exception to this is the value 0. It is fine to have a rate limit but not an attack detect threshold of 0.

Format	<code>no arp-guard attack-threshold {per-src-ip per-src-mac per-port}</code>
Mode	Global Config

`show arp-guard summary`

M4250

M4350

This command displays the ARP Guard feature configuration for all interfaces, for a specific interface, or for a specific LAG (port-channel). To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument `slot/port`.
- For an M4350 series switch, use the argument `unit/slot/port`, as shown in the command format.

Format	<code>show arp-guard summary [interface <i>unit/slot/port</i> lag <i>lag-number</i>]</code>

Mode	Privileged EXEC

Command example:

The following example shows the ARP Guard configuration for all interfaces.

```
(NETGEAR Switch) #show arp-guard summary
```

(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)

Interface	AdminMode	Status	Rate-limit (in pps)	Attack-threshold (in pps)
Global	Disabled	Disabled	10/50/200	50/100/400
1/0/2	Enabled	Enabled	25/50/150	50/100/200
1/0/5	Enabled	Enabled	15/25/50	50/50/100
1/0/6	Enabled	Enabled	50/50/150	100/100/200
1/0/18	Enabled	Enabled	50/50/150	100/100/200

Command example:

The following example shows the ARP Guard configuration for interface 1/0/2.

```
(NETGEAR Switch) #show arp-guard summary
```

(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)

Interface	Status	Rate-limit (in pps)	Attack-threshold (in pps)
1/0/2	Enabled	25/50/150	50/100/200

show arp-guard statistics**M4250****M4350**

This command displays all the ARP Guard statistics for all interfaces, including the global statistics, or the statistics for a specific interface or a specific LAG (port-channel). To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show arp-guard statistics {all interface <i>unit/slot/port</i> lag <i>lag-number</i>}</code>

Mode	Privileged EXEC

Command example:

The following example shows the ARP Guard statistics for interface 1/0/2.

```
(NETGEAR Switch) #show arp-guard statistics interface 1/0/2
```

```
Interface 1/0/2
```

```
Rate limit hit count on the interface..... 10
Rate limit hit count per Host source IP..... 12
Rate limit hit count per Host source MAC..... 3
Attacks detected on the interface..... 7
Attacks detected per Host source IP..... 15
Attacks detected per Host source MAC..... 14
```

Command example:

The following example shows the ARP Guard statistics for interface 1/0/2.

```
(NETGEAR Switch) #show arp-guard statistics interface all
```

```
Global Statistics
```

```
Rate limit hit count on all interfaces..... 23
Rate limit hit count per Host source IP..... 14
Rate limit hit count per Host source MAC..... 11
Attacks detected on all interfaces..... 22
Attacks detected per Host source IP..... 19
Attacks detected per Host source MAC..... 32
```

```
Interface 1/0/2
```

```
Rate limit hit count on the interface..... 13
Rate limit hit count per Host source IP..... 2
Rate limit hit count per Host source MAC..... 8
Attacks detected on the interface..... 15
Attacks detected per Host source IP..... 4
Attacks detected per Host source MAC..... 18
```

```
Interface 1/0/16
```

```
Rate limit hit count on the interface..... 10
Rate limit hit count per Host source IP..... 12
Rate limit hit count per Host source MAC..... 3
Attacks detected on the interface..... 7
Attacks detected per Host source IP..... 15
Attacks detected per Host source MAC..... 14
```

show arp-guard attack history

M4250**M4350**

Use this command to display the ARP-Guard attack events history for a host that is identified by the source IP address or source MAC address, or by port. If you use the **all** keyword, the entire ARP-Guard attack events history is displayed.

Format	show arp-guard attack history {all per-src-ip per-src-mac per-port}
Mode	Privileged EXEC
Term	Definition
all	Displays the ARP-Guard attack event history by hosts identified by source IP address., source MAC address, and port.
per-src-ip	Displays the ARP-Guard attack events history by hosts identified by source IP address.
per-src-mac	Displays the ARP-Guard attack events history by hosts identified by source MAC address.
per-port	Displays the ARP-Guard attack events history by port.

Command example:

The following example shows the ARP Guard attack events history per host based on the source IP address.

```
(NETGEAR Switch) #show arp-guard attack history per-src-ip
```

VLAN	Interface	IP address	Timestamp
----	-----	-----	-----
1	1/0/2	4.5.5.17	0h 17m 26s
10	1/0/14	7.6.14.2	0h 38m 13s
20	1/0/9	5.58.12.23	0h 54m 49s

Command example:

The following example shows the ARP Guard attack events history per host based on the source MAC address.

```
(NETGEAR Switch) #show arp-guard attack history per-src-mac
```

VLAN	Interface	MAC address	Timestamp
----	-----	-----	-----
1	1/0/5	00:1a:b3:c9:46:03	0h 12m 28s
10	1/0/26	00:2c:67:f4:33:a5	0h 30m 06s
20	1/0/13	00:d8:a5:23:b4:c9	0h 42m 37s

Command example:

The following example shows the ARP Guard attack events history per port.

```
(NETGEAR Switch) #show arp-guard attack history per-port
```

```
VLAN Interface  Timestamp
----
1      1/0/5      0h 22m 07s
10     1/0/26     0h 47m 19s
20     1/0/13     0h 12m 33s
```

clear arp-guard statistics

M4250

M4350

Use this command to clear the ARP guard statistics on a specific interface or lag, or for all interfaces. When you select the **all** keyword, the global statistics are cleared too.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	clear arp-guard statistics {all interface <i>unit/slot/port</i> lag <i>lag-num</i> }

Mode	Privileged EXEC

Parameter	Description

all	Clears the ARP guard statistics and global statistics for all interfaces.

<i>unit/slot/port</i>	Clear the ARP guard statistics for the specified interface.

<i>lag-num</i>	Clear the ARP guard statistics for the specified LAG.

clear arp-guard attack history

M4250

M4350

Use this command to clear the ARP guard attack history for the per-host source IP address category, per-host source MAC address category, or per-port category, or for all three of these categories.

Format	clear arp-guard attack history {all per-src-ip per-src-mac per-port}

Mode	Privileged EXEC

Parameter	Description
all	Clears the ARP guard attack history for all three categories (per-source IP address, per-source MAC address, and per-port).
per-src-ip	Clears the ARP guard attack history for the per-source IP address category.
per-src-mac	Clears the ARP guard attack history for the per-source MAC address category.
per-port	Clears the ARP guard attack history for the per-port category.

MVR Commands

Internet Group Management Protocol (IGMP) Layer 3 is widely used for IPv4 network multicasting. In Layer 2 networks, IGMP uses resources inefficiently. For example, a Layer 2 switch multicast traffic to all ports, even if there are receivers connected to only a few ports.

To address this problem, the IGMP Snooping protocol was developed. The problem still appears, though, when receivers are in different VLANs.

Multicast VLAN registration (MVR) is intended to solve the problem of receivers in different VLANs. It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over a Layer 2 network with IGMP snooping.

mvr

M4250

M4350

This command enables MVR.

Default	Disabled
Format	mvr
Mode	Global Config Interface Config

no mvr

This command disables MVR.

Format	no mvr
Mode	Global Config Interface Config

mvr group

M4250

M4350

This command adds an MVR membership group. *A.B.C.D* is the IP multicast group being added.

The count is the number of incremental multicast groups being added (the first multicast group is A.B.C.D). If a count is not specified, only one multicast group is added.

Format	<code>mvr group A.B.C.D [count]</code>
Mode	Global Config

no mvr group

This command removes the MVR membership group.

Format	<code>no mvr group A.B.C.D [count]</code>
Mode	Global Config

mvr mode

M4250

M4350

This command changes the MVR mode type. If the mode is set to compatible, the switch does not learn multicast groups; they need to be configured by the operator as the protocol does not forward joins from the hosts to the router. To operate in this mode, the IGMP router needs to be statically configured to transmit all required multicast streams to the MVR switch. If the mode is set to dynamic, the switch learns existing multicast groups by snooping the IGMP queries from the router on source ports and forwarding the IGMP joins from the hosts to the IGMP router on the multicast VLAN (with appropriate translation of the VLAN ID).

Default	Compatible
Format	<code>mvr mode {compatible dynamic}</code>
Mode	Global Config

no mvr mode

This command sets the mode type to the default value.

Format	<code>no mvr mode</code>
Mode	Global Config

mvr querytime

M4250

M4350

This command sets the MVR query response time in deciseconds. The time is in the range 1–100 deciseconds (one decisecond is one tenth of a second).

Default	5
Format	<code>mvr querytime deciseconds</code>
Mode	Global Config

no mvr querytime

This command sets the MVR query response time to the default value.

Format	<code>no mvr querytime</code>
Mode	Global Config

mvr vlan

M4250

M4350

This command sets the MVR multicast VLAN.

Default	1
Format	<code>mvr vlan vlan-id</code>
Mode	Global Config

no mvr vlan

This command sets the MVR multicast VLAN to the default value.

Format	<code>no mvr vlan</code>
Mode	Global Config

mvr immediate

M4250

M4350

This command enables MVR immediate leave mode. MVR provides two modes of operating with the IGMP Leave messages: normal leave and immediate leave.

- In normal leave mode, when a leave is received, the general IGMP query is sent from a Layer 2 switch to the receiver port, where the leave was received. Then reports are received from other interested hosts that are also connected to that port, for example, using hub.
- In immediate leave mode, when a leave is received, the switch is immediately reconfigured not to forward a specific multicast stream to the port where a message is received. This mode is used only for ports where only one client might be connected.

Default	Disabled
Format	<code>mvr immediate</code>
Mode	Interface Config

no mvr immediate

This command sets the MVR multicast VLAN to the default value.

Format	<code>no mvr immediate</code>
Mode	Interface Config

mvr type

M4250

M4350

This command sets the MVR port type. When a port is set as source, it is the port to which the multicast traffic flows using the multicast VLAN. When a port is set to receiver, it is the port where a listening host is connected to the switch.

Default	none
Format	<code>mvr type {receiver source}</code>
Mode	Interface Config

no mvr type

Use this command to set the MVR port type to none.

Format	no mvr type

Mode	Interface Config

mvr vlan group

M4250

M4350

Use this command to include the port in the specific MVR group. The *multicast-vlan* argument represents is the multicast VLAN, and *A.B.C.D* the IP multicast group.

Format	mvr vlan <i>multicast-vlan</i> group <i>A.B.C.D</i>

Mode	Interface Config

no mvr vlan

Use this command to exclude the port from the specific MVR group.

Format	no mvr vlan <i>multicast-vlan</i> group <i>A.B.C.D</i>

Mode	Interface Config

show mvr

M4250

M4350

This command displays global MVR settings.

Format	show mvr

Mode	Privileged EXEC

The following table explains the output parameters.

Term	Definition
MVR Running	MVR running state. It can be enabled or disabled.
MVR multicast VLAN	Current MVR multicast VLAN. It can be in the range from 1 to 4094.
MVR Max Multicast Groups	The maximum number of multicast groups supported by MVR.
MVR Current multicast groups	The current number of MVR groups allocated.

Term	Definition
MVR Query response time	The current MVR query response time.
MVR Mode	The current MVR mode. It can be compatible or dynamic.

Command example:

```
(NETGEAR Switch)#show mvr
MVR Running..... TRUE
MVR multicast VLAN..... 1200
MVR Max Multicast Groups..... 256
MVR Current multicast groups..... 1
MVR Global query response time..... 10 (tenths of sec)
MVR Mode..... compatible
```

show mvr members**M4250****M4350**

This command displays the MVR membership groups allocated. *A.B.C.D* is a valid multicast address in IPv4 dotted notation.

Format	<code>show mvr members [A.B.C.D]</code>
Mode	Privileged EXEC

The following table describes the output parameters.

Term	Definition
MVR Group IP	MVR group multicast IP address.
Status	The status of the specific MVR group. It can be active or inactive.
Members	The list of ports that participates in the specified MVR group.

Command example:

```
(NETGEAR Switch)#show mvr members
MVR Group IP      Status      Members
-----
224.1.1.1         INACTIVE    0/1, 0/2, 0/3

(switch)#show mvr members 224.1.1.1
MVR Group IP      Status      Members
-----
224.1.1.1         INACTIVE    0/1, 0/2, 0/3
```

show mvr interface

M4250

M4350

This command displays the MVR-enabled interfaces configuration. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show mvr interface [<i>unit/slot/port</i> [members [<i>vlan multicast-vlan</i>]]]

Mode	Privileged EXEC

The following table explains the output parameters.

Term	Description
Port	Interface number
Type	The MVR port type. It can be none, receiver, or source type.
Status	The interface status. It consists of two characteristics: • active or inactive indicates whether the port is forwarding. • inVLAN or notInVLAN indicates whether the port is part of any VLAN.
Immediate Leave	The state of immediate mode. It can be enabled or disabled.

Command example:

```
(NETGEAR Switch)#show mvr interface
```

Port	Type	Status	Immediate Leave
0/9	RECEIVER	ACTIVE/inVLAN	DISABLED

```
(switch)#show mvr interface 0/9
```

```
Type: RECEIVER Status: ACTIVE Immediate Leave: DISABLED
```

```
(switch)#show mvr interface 0/23 members
```

```
235.0.0.1 STATIC ACTIVE
```

```
(switch)#show mvr interface 0/23 members vlan 12
```

```
235.0.0.1 STATIC ACTIVE
```

```
235.1.1.1 STATIC ACTIVE
```

show mvr traffic

M4250**M4350**

This command displays global MVR statistics.

Format	show mvr traffic
Mode	Privileged EXEC

The following table explains the output parameters.

Term	Definition
IGMP Query Received	Number of received IGMP queries
IGMP Report V1 Received	Number of received IGMP reports V1
IGMP Report V2 Received	Number of received IGMP reports V2
IGMP Leave Received	Number of received IGMP leaves
IGMP Query Transmitted	Number of transmitted IGMP queries
IGMP Report V1 Transmitted	Number of transmitted IGMP reports V1
IGMP Report V2 Transmitted	Number of transmitted IGMP reports V2
IGMP Leave Transmitted	Number of transmitted IGMP leaves
IGMP Packet Receive Failures	Number of failures on receiving the IGMP packets
IGMP Packet Transmit Failures	Number of failures on transmitting the IGMP packets

Command example:

```
(NETGEAR Switch)#show mvr traffic
```

```
IGMP Query Received..... 2
IGMP Report V1 Received..... 0
IGMP Report V2 Received..... 3
IGMP Leave Received..... 0
IGMP Query Transmitted..... 2
IGMP Report V1 Transmitted..... 0
IGMP Report V2 Transmitted..... 3
IGMP Leave Transmitted..... 1
IGMP Packet Receive Failures..... 0
IGMP Packet Transmit Failures..... 0
```

debug mvr trace

M4250

M4350

This command enables MVR debug tracing. By default, MVR debug tracing is disabled.

Format	debug mvr trace
Mode	Privileged EXEC

no debug mvr trace

This command disables MVR debug tracing.

Format	no debug mvr trace
Mode	Privileged EXEC

debug mvr packet

M4250

M4350

This command enables debug tracing of MVR packets on the receiving side, transmitting side, or both sides. By default, debug tracing of MVR packets is enabled.

Format	debug mvr packet [receive transmit]
Mode	Privileged EXEC

no debug mvr packet

This command disables debug tracing of MVR packets on the receiving side, transmitting side, or both sides.

Format	no debug mvr packet [receive transmit]
Mode	Privileged EXEC

IGMP Snooping Configuration Commands

This section describes the commands you use to configure IGMP snooping. The switch supports IGMP Versions 1, 2, and 3. The IGMP snooping feature can help conserve bandwidth because it allows the switch to forward IP multicast traffic only to connected hosts that request multicast traffic. IGMPv3 adds source filtering capabilities to IGMP versions 1 and 2.

Note: This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

set igmp

M4250

M4350

This command enables IGMP Snooping on the system (Global Config Mode), an interface, or a range of interfaces. This command can also enable IGMP snooping on a particular VLAN (VLAN Config mode, also referred to as VLAN Database mode) and can enable IGMP snooping on all interfaces participating in a VLAN.

If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

The IGMP application supports the following activities:

- Validation of the IP header checksum (as well as the IGMP header checksum) and discarding of the frame upon checksum error.
- Maintenance of the forwarding table entries based on the MAC address versus the IP address.
- Filters unknown IPv4 multicast packets on a VLAN if IGMP snooping is enabled, with the exception of group addresses in the range 224.0.0.x. These control packets are always flooded to all ports in the VLAN.

Format	set igmp
Mode	Global Config Interface Config
Default	Enabled for VLAN 1; Disabled for other VLANs.
Format	set igmp [vlan-id]
Mode	VLAN Config (also referred to as VLAN Database)

no set igmp

This command disables IGMP Snooping on the system, an interface, a range of interfaces, or a VLAN.

Format	no set igmp
Mode	Global Config Interface Config
Format	no set igmp [vlan-id]
Mode	VLAN Config (also referred to as VLAN Database)

set igmp interfacemode

M4250

M4350

This command enables IGMP Snooping on all interfaces. If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

Default	Disabled
Format	set igmp interfacemode
Mode	Global Config

no set igmp interfacemode

This command disables IGMP Snooping on all interfaces on the switch at the same time. It is disabled by default. This command does not take effect on the interface where routing is enabled or is a member of a port-channel (LAG). Disable routing on the interface before setting IGMP Snooping. The interface that is a member of a port-channel (LAG) must be removed before setting IGMP Snooping

Default	Disabled
Format	no set igmp interfacemode
Mode	Global Config

set igmp fast-leave

M4250

M4350

This command enables or disables IGMP Snooping fast-leave on a selected interface, a range of interfaces, or a VLAN.

When you enable fast-leave, the switch immediately removes a layer 2 LAN interface from its forwarding table if the following situation occurs:

1. The switch does not send MAC-based general queries to the layer 2 LAN interface.
2. The switch receives an IGMP leave message for the associated multicast group.

Enable fast-leave only on VLANs for which a single host is connected to each layer 2 LAN interface. Doing so prevents the inadvertent dropping of other hosts that are connected to the same layer 2 LAN interface but are still interested in receiving multicast traffic that is directed to the multicast group.

Fast-leave processing is supported for IGMPv2 hosts only.

Format	<code>set igmp fast-leave</code>
Mode	Interface Config

Format	<code>set igmp fast-leave <i>vlan-id</i></code>
Mode	VLAN Config (also referred to as VLAN Database)

no set igmp fast-leave

This command disables IGMP Snooping fast-leave admin mode on a selected interface.

Format	<code>no set igmp fast-leave</code>
Mode	Interface Config

Format	<code>no set igmp fast-leave <i>vlan-id</i></code>
Mode	VLAN Config (also referred to as VLAN Database)

set igmp fast-leave auto-assignment

M4250

M4350

This command globally enables the automatic assignment of fast-leave for all ports and LAGs.

On the switch, Rapid Spanning Tree Protocol (RSTP) is the default network protocol for STP. RSTP functions at port level. Each port starts up as an edge port and functions in that

capacity until it receives an RSTP BPDU from a neighbor device. An edge port does not participate in STP and is meant to be connected to end devices or hosts on which STP is not enabled. However, if a port receives an RSTP BPDU, the port stops functioning as an edge port and starts participating in STP.

Consequently, as long as the port functions as an edge port, IGMP Snooping fast-leave is enabled. If a port receives an RSTP BPDU and stops functioning as an edge port, IGMP Snooping fast-leave is also disabled on the port.

The **set igmp fast-leave auto-assignment** command controls the fast-leave operational state, but not the configured value. On a port, a dynamically-assigned operational value for fast-leave overrides a configured value for fast-leave.

The **set igmp fast-leave auto-assignment** command does the following:

- It overrides the configured port level fast-leave mode, which is disabled by default.
- It does not modify the VLAN configuration for fast-leave mode.

Between a port and a VLAN that is configured for that port, IGMP Snooping gives precedence to the fast-leave mode for the port.

You can display the operational status of IGMP Snooping fast-leave at port level by using the **show igmpsnooping fast-leave** command (see [show igmpsnooping fast-leave on page 769](#)).

Default	Enabled
Format	set igmp fast-leave auto-assignment
Mode	Global Config

no set igmp fast-leave auto-assignment

This command globally disables the automatic assignment of fast-leave for all ports and LAGs.

Format	no set igmp fast-leave auto-assignment
Mode	Global Config

set igmp groupmembership-interval

M4250

M4350

This command sets the IGMP group membership interval time on a VLAN, one interface, a range of interfaces, or all interfaces. The group membership interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular

interface before deleting the interface from the entry. This value must be greater than the IGMPv3 maximum response time value. The range is 2 to 3600 seconds.

Default	260 seconds
Format	<code>set igmp groupmembership-interval <i>seconds</i></code>
Mode	Interface Config Global Config

Default	260 seconds
Format	<code>set igmp groupmembership-interval <i>vlan-id seconds</i></code>
Mode	VLAN Config (also referred to as VLAN Database)

`no set igmp groupmembership-interval`

This command sets the IGMPv3 group membership interval time to the default value.

Format	<code>no set igmp groupmembership-interval</code>
Mode	Interface Config Global Config

Format	<code>no set igmp groupmembership-interval <i>vlan-id</i></code>
Mode	VLAN Config (also referred to as VLAN Database)

`set igmp maxresponse`

M4250

M4350

This command sets the IGMP maximum response time for the system, on a particular interface or VLAN, or on a range of interfaces. The maximum response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP query Interval time value. The range is 1 to 300 seconds.

Default	600 seconds
Format	<code>set igmp maxresponse <i>seconds</i></code>
Mode	Global Config Interface Config
Default	600 seconds

Format	<code>set igmp maxresponse <i>vlan-id</i> <i>seconds</i></code>

Mode	VLAN Config (also referred to as VLAN Database)

`no set igmp maxresponse`

This command sets the max response time (on the interface or VLAN) to the default value.

Format	<code>no set igmp maxresponse</code>

Mode	Global Config Interface Config

Format	<code>no set igmp maxresponse <i>vlan-id</i></code>

Mode	VLAN Config (also referred to as VLAN Database)

`set igmp mcartexpiretime`

M4250

M4350

This command sets the multicast router present expiration time. The time is set for the system, on a particular interface or VLAN, or on a range of interfaces. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite time-out, that is, no expiration.

Default	0

Format	<code>set igmp mcartexpiretime <i>seconds</i></code>

Mode	Global Config Interface Config

Default	0

Format	<code>set igmp mcartexpiretime <i>vlan-id</i> <i>seconds</i></code>

Mode	VLAN Config (also referred to as VLAN Database)

`no set igmp mcartexpiretime`

This command sets the multicast router present expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

Format	<code>no set igmp mcartexpiretime</code>

Mode	Global Config Interface Config

Format	<code>no set igmp mcarttexpiretime <i>vlan-id</i></code>

Mode	VLAN Config (also referred to as VLAN Database)

set igmp mrouter

M4250

M4350

This command configures the VLAN ID that has the multicast router mode enabled.

Format	<code>set igmp mrouter <i>vlan-id</i></code>

Mode	Interface Config

no set igmp mrouter

This command disables multicast router mode for a particular VLAN ID.

Format	<code>no set igmp mrouter <i>vlan-id</i></code>

Mode	Interface Config

set igmp mrouter interface

M4250

M4350

This command configures the interface or range of interfaces as a multicast router interface. When configured as a multicast router interface, the interface is treated as a multicast router interface in all VLANs.

Default	disabled

Format	<code>set igmp mrouter interface</code>

Mode	Interface Config

no set igmp mrouter interface

This command disables the status of the interface as a statically configured multicast router interface.

Format	<code>no set igmp mrouter interface</code>

Mode	Interface Config

set igmp flood-report

M4250**M4350**

This command lets the switch forward IGMP Join/Leave PDUs to all other ports, either globally or in a VLAN. These are IGMP Join/Leave PDUs that the switch receives from a host that is connected to a downstream port.

Format	<code>set igmp flood report</code>
Mode	Global Config
Format	<code>set igmp flood report <i>vlan-id</i></code>
Mode	VLAN Config (also referred to as VLAN Database)

no set igmp flood-report

This command prevents the switch from forwarding IGMP Join/Leave PDUs to all other ports, either globally or in a VLAN.

Format	<code>no set igmp flood report</code>
Mode	Global Config
Format	<code>no set igmp flood report <i>vlan-id</i></code>
Mode	VLAN Config (also referred to as VLAN Database)

set igmp exclude-mrouter-intf

M4250**M4350**

This command lets the switch forward IGMP Join/Leave PDUs to an upstream multicast router interface. These are IGMP Join/Leave PDUs that the switch receives from a host that is connected to a downstream port. In addition, the switch forwards a multicast data stream to an upstream mrouter interface only if that port already received an IGMPv1 or IGMPv2 membership message. This behavior does not apply to IGMPv3 membership.

Format	<code>set igmp exclude-mrouter-intf</code>
Mode	Global Config
Format	<code>set igmp exclude-mrouter-intf <i>vlan-id</i></code>
Mode	VLAN Config (also referred to as VLAN Database)

A designated mrouter port that is either detected dynamically or manually configured forwards the following information to the upstream router:

- All IGMPv1, IGMPv2, and IGMPv3 PDUs.
- All unknown multicast streams, that is, streams for which the switch did not receive IGMP membership.
- All known multicast streams, that is, streams for which switch did receive IGMP membership and for which it updated its hardware MFDB table.

Use the **set igmp exclude-mrouter-intf** command to prevent the switch from forwarding unknown and known IGMPv1 and IGMPv2 multicast streams *unless* the downstream port received an IGMPv1 or IGMPv2 membership. The switch still forward all IGMPv1, IGMPv2, and IGMPv3 PDUs.

```
no set igmp exclude-mrouter-intf
```

This command prevents the switch from forwarding IGMP Join/Leave PDUs to an upstream multicast router interface.

Format	<code>no igmp exclude-mrouter-intf</code>
Mode	Global Config

Format	<code>no igmp exclude-mrouter-intf vlan-id</code>
Mode	VLAN Config (also referred to as VLAN Database)

set igmp report-suppression

M4250

M4350

Use this command to suppress the IGMP reports on a VLAN. To optimize the number of reports traversing the network with no added benefits, a Report Suppression mechanism is implemented. When more than one client responds to an MGMT query for the same Multicast Group address within the max-response-time, only the first response is forwarded to the query and others are suppressed at the switch.

Default	Disabled

Format	<code>set igmp report-suppression vlan-id</code>
Mode	VLAN Config (also referred to as VLAN Database)

Parameter	Description
vlan-id	A valid VLAN ID. Range is 1 to 4093.

Command example:

```
(NETGEAR Switch) #vlan database
(NETGEAR Switch) (Vlan)#set igmp report-suppression ?
```

```
<1-4093>          Enter VLAN ID.
```

```
(NETGEAR Switch) (Vlan)#set igmp report-suppression 1
```

```
no set igmp report-suppression
```

Use this command to return the system to the default.

Format	no set igmp report-suppression
Mode	VLAN Config (also referred to as VLAN Database)

```
set igmp header-validation
```

M4250

M4350

This command enables IGMP IP header validation.

If IGMP IP header validation is enabled, three fields, TTL (Time To Live), ToS (Type of Service), and Router Alert options, are checked. The actual validated fields depend on the IGMP version. The TTL field is validated in all the versions (IGMPv1, IGMPv2, and IGMPv3). The Router Alert field is validated in IGMPv2 and IGMPv3. The ToS field is validated only in IGMP version3.

Default	Enabled
Format	set igmp header-validation
Mode	Global Config

```
no set igmp header-validation
```

This command disables the IGMP IP header validation.

Format	no set igmp header-validation
Mode	Global Config

set igmp-plus (Global Config)

M4250

M4350

This command enables all of the following global IGMP Snooping configuration commands:

- **set igmp**
- **set igmp querier**
- **set igmp flood-report**
- **set igmp exclude-mrouter-intf**
- **set igmp fast-leave auto-assignment**

Default	Enabled
Format	set igmp-plus
Mode	Global Config

no set igmp-plus (Global Config)

This command disables all of the following global IGMP Snooping configuration commands:

- **set igmp**
- **set igmp querier**
- **set igmp flood-report**
- **set igmp exclude-mrouter-intf**
- **set igmp fast-leave auto-assignment**

Format	no set igmp-plus
Mode	Global Config

set igmp-plus (VLAN Config)

M4250

M4350

After you enable the **set igmp-plus** command, you can enable the **set igmp-plus vlan** command to enable all of the following global IGMP Snooping configuration commands at the VLAN level for a particular VLAN:

- **set igmp *vlan-id***
- **set igmp exclude-mrouter-intf *vlan-id***
- **set igmp fast-leave *vlan-id***
- **set igmp flood-report *vlan-id***

- **set igmp querier** *vlan-id*
- **set igmp querier election participate** *vlan-id*

The *vlan* argument in the **set igmp-plus** *vlan-id* command can be a VLAN from 1 to 4093.

Default	Enabled for VLAN 1
Format	<code>set igmp-plus <i>vlan-id</i></code>
Mode	VLAN Config (also referred to as VLAN Database)

`no set igmp-plus` (VLAN Config)

This command disables all of the following global IGMP Snooping configuration commands at the VLAN level for a particular VLAN:

- **set igmp** *vlan-id*
- **set igmp exclude-mrouter-intf** *vlan-id*
- **set igmp fast-leave** *vlan-id*
- **set igmp flood-report** *vlan-id*
- **set igmp querier** *vlan-id*
- **set igmp querier election participate** *vlan-id*

The *vlan* argument in the **no set igmp-plus** *vlan-id* command can be a VLAN from 1 to 4093.

Format	<code>no set igmp-plus <i>vlan-id</i></code>
Mode	VLAN Config (also referred to as VLAN Database)

`show igmpsnooping`

M4250

M4350

This command displays IGMP Snooping information for an interface, VLAN, or LAG. Configured information is displayed whether or not IGMP Snooping is enabled. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show igmpsnooping [<i>unit/slot/port</i> <i>vlan-id</i> <i>lag lag-id</i>]</code>
Mode	Privileged EXEC

If you do not use the optional arguments *unit/slot/port*, *vlan-id*, or *lag-id* the command displays the following information.

Term	Definition
Admin Mode	Indicates whether or not IGMP Snooping is active on the switch.
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.
Interface Enabled for IGMP Snooping	The list of interfaces on which IGMP Snooping is enabled.
VLANs Enabled for IGMP Snooping	The list of VLANs on which IGMP Snooping is enabled.

When you specify the *unit/slot/port* values or a *lag-id* value, the following information displays.

Term	Definition
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the interface.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the interface.
Group Membership Interval (secs)	The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry. This value may be configured.
Maximum Response Time (secs)	The amount of time the switch waits after it sends a query on an interface because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time (secs)	The amount of time to wait before removing an interface from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.
Report Suppression Mode	Indicates whether IGMP reports (set by the command set igmp report-suppression on page 764) in enabled or not.
Report Flood Mode	Indicates whether the IGMP Report Flood Mode is enabled or not.
Exclude Mrouter Interface Mode	Indicates whether the Exclude Mrouter Interface Mode is enabled or not.
IGMP-PLUS	Indicates whether IGMP Plus is globally enabled or not.

When you specify a value for *vlan-id*, the following information displays.

Term	Definition
VLAN ID	The VLAN ID.
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the VLAN.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the VLAN.
Group Membership Interval (secs)	The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry. This value may be configured.

Term	Definition
Maximum Response Time (secs)	The amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time (secs)	The amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.
Report Suppression Mode	Indicates whether IGMP reports (set by the command set igmp report-suppression on page 764) in enabled or not.
Report Flood Mode	Indicates whether the IGMP Report Flood Mode is enabled or not.
Exclude Mrouter Interface Mode	Indicates whether the Exclude Mrouter Interface Mode is enabled or not.
IGMP-PLUS	Indicates whether IGMP Plus is enabled for the VLAN or not.

Command example:

```
(NETGEAR switch) #show igmpsnooping 1
```

```
VLAN ID..... 1
IGMP Snooping Admin Mode..... Enabled
Fast Leave Mode..... Enabled
Group Membership Interval (secs)..... 600
Max Response Time (secs)..... 120
Multicast Router Expiry Time (secs)..... 300
Report Suppression Mode..... Disabled
Report Flood Mode..... Enabled
Exclude Mrouter Interface Mode..... Enabled
IGMP-Plus..... Enabled
```

show igmpsnooping fast-leave**M4250****M4350**

This command displays the status of IGMP Snooping fast-leave for ports.

Format	show igmpsnooping fast-leave

Mode	Privileged EXEC

Term	Definition
Interface	The physical port or LAG for which the IGMP Snooping fast-leave information is displayed.

Term	Definition
Fast-Leave Admin Mode	Indicates whether IGMP Snooping fast-leave is enabled or disabled on the physical port or LAG.
Fast-Leave Operational Mode	Indicates the operational status of IGMP Snooping fast-leave on the physical port or LAG.

Command example:

```
(NETGEAR switch) #show igmpsnooping fast-leave
```

```
Fast Leave Auto-Assignment Mode..... Enable
```

Interface	Fast-Leave Admin Mode	Fast-Leave Operational Mode
-----	-----	-----
1/1/1	Disable	Disable
1/1/2	Disable	Disable
1/1/3	Disable	Disable
1/1/4	Disable	Disable

show igmpsnooping group**M4250****M4350**

This command displays the source and group IP addresses and the corresponding MAC addresses that the switch detected through IGMP Snooping on a VLAN, interface, or LAG.

If you do not specify a specific VLAN, interface, or LAG, the command output display all detected IGMP Snooping entries on all VLANs, interfaces, and LAGs on the switch. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show igmpsnooping group [vlan-id unit/slot/port lag lag-id]</code>

Mode	Privileged EXEC

Term	Definition
VLAN ID	The VLAN ID to which the host forwards IGMP member join requests.
Subscriber	The IP address and MAC address of the host
MC Group	The IP address and MAC address of the multicast group.
Interface	The interface on which the IGMP member join request is detected.

Term	Definition
Type	The IGMP version.
Timeout (Sec)	The period in seconds after which the most recent host update expires. The timer is reset if an IGMP member join request is received for the multicast group.

Command example:

```
(NETGEAR switch) #show igmpsnooping group
```

VLAN ID	Subscriber	MC Group	Interface	Type	Timeout (Sec)
1	1.1.1.6/00:00:00:00:00:06	224.1.1.6/01:00:5E:01:01:06	1/0/16	IGMPv2	252
1	1.1.1.8/00:00:00:00:00:08	224.1.1.6/01:00:5E:01:01:06	1/0/18	IGMPv2	256
	1.1.1.9/00:00:00:00:00:09				
	1.1.1.10/00:00:00:00:00:0A				
	1.1.1.11/00:00:00:00:00:0B				
	1.1.1.12/00:00:00:00:00:0C				
1	1.1.1.9/00:00:00:00:00:09	224.1.1.7/01:00:5E:01:01:07	1/0/18	IGMPv2	181
1	1.1.1.10/00:00:00:00:00:0A	224.1.1.8/01:00:5E:01:01:08	1/0/18	IGMPv2	182
1	1.1.1.11/00:00:00:00:00:0B	224.1.1.9/01:00:5E:01:01:09	1/0/18	IGMPv2	183
1	1.1.1.12/00:00:00:00:00:0C	224.1.1.10/01:00:5E:01:01:0A	1/0/18	IGMPv2	184

In the command output example, both multicast group IP addresses and interfaces are used:

- The information on the 1st and 2nd lines is for the same group (224.1.1.6, with different sources) but detected on different interfaces (1/0/16 and 1/0/18) and therefore displayed on two separate lines.
- The information on the 2nd line is for a single group (224.1.1.6) on interface 1/0/18, but includes subscriptions from different hosts. All the host IP addresses are combined on the same line.
- The information on the 3rd, 4th, 5th, and 6th lines are for different multicast groups but detected on the same interface. Because the group IP addresses are different, the information is displayed on different lines.

show igmpsnooping mrouter interface

M4250

M4350

This command displays interfaces on which multicast routers are detected. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format show igmpsnooping mrouter interface {unit/slot/port | all}

Mode Privileged EXEC

Term	Definition
Interface	The port for which multicast router information is displayed.
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.
VLAN ID	The list of VLANs of which the interface is a member.

show igmpsnooping mrouter vlan

M4250

M4350

This command displays VLAN interfaces on which multicast routers are detected. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show igmpsnooping mrouter vlan {vlan-id interface unit/slot/port}</code>
Mode	Privileged EXEC

Term	Definition
Interface	The port on which multicast router information is displayed.
VLAN ID	The list of VLANs of which the interface is a member.

show igmpsnooping ssm

M4250

M4350

This command displays information about Source Specific Multicasting (SSM) by entry, group, or statistics. SSM delivers multicast packets to receivers that originated from a source address specified by the receiver. SSM is only available with IGMPv3 and MLDv2.

Format	<code>show igmpsnooping ssm {entries groups stats}</code>
Mode	Privileged EXEC

show mac-address-table igmpsnooping

M4250

M4350

This command displays the IGMP Snooping entries in the MFDB table.

Format	show mac-address-table igmpsnooping
Mode	Privileged EXEC
Term	Definition
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of the entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol).
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

IGMP Snooping Querier Commands

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 will stop forwarding multicasts to the port where the end device is located.

This section describes commands used to configure and display information on IGMP Snooping Queriers on the network and, separately, on VLANs.

Note: This note clarifies the prioritization of MGLD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

set igmp querier

M4250

M4350

Use this command to enable IGMP Snooping Querier on the system, using Global Config mode, or on a VLAN. Using this command, you can specify the IP Address that the Snooping Querier switch should use as the source address while generating periodic queries.

If a VLAN has IGMP Snooping Querier enabled and IGMP Snooping is operationally disabled on it, IGMP Snooping Querier functionality is disabled on that VLAN. IGMP Snooping functionality is re-enabled if IGMP Snooping is operational on the VLAN.

Note: The Querier IP Address assigned for a VLAN takes preference over global configuration.

The IGMP Snooping Querier application supports sending periodic general queries on the VLAN to solicit membership reports.

Default	Enabled in Global Config mode with default VLAN 1
Format	set igmp querier [address <i>ipaddress</i>]
Mode	Global Config
Default	Enabled in Global Config mode with default VLAN 1
Format	set igmp querier [<i>vlan-id</i>] [address <i>ipaddress</i>]
Mode	VLAN Mode

no set igmp querier

Use this command to disable IGMP Snooping Querier on the system. Use the optional **address** parameter to reset the querier address to 0.0.0.0.

Format	no set igmp querier [address]
Mode	Global Config
Format	no set igmp querier [<i>vlan-id</i>] [address]
Mode	VLAN Mode

set igmp querier query-interval

M4250**M4350**

Use this command to set the IGMP querier query interval time. It is the period in seconds, from 1–1800 seconds, that the switch waits before sending another general query.

Default	60 seconds
Format	set igmp querier query-interval <i>seconds</i>
Mode	Global Config

no set igmp querier query-interval

Use this command to set the IGMP querier query interval time to its default value.

Format	no set igmp querier query-interval
Mode	Global Config

set igmp querier timer expiry

M4250**M4350**

Use this command to set the IGMP querier timer expiration period in seconds, from 60–300 seconds. This is the period that the switch remains in non-querier mode after it has discovered a multicast querier in the network.

Default	60 seconds
Format	set igmp querier timer expiry <i>seconds</i>
Mode	Global Config

no set igmp querier timer expiry

Use this command to set the IGMP querier timer expiration period to its default value.

Format	no set igmp querier timer expiry
Mode	Global Config

set igmp querier version

M4250

M4350

Use this command to set the IGMP version of the query that the snooping switch sends periodically.

Default	1
Format	set igmp querier version {1 2 3}
Mode	Global Config

no set igmp querier version

Use this command to set the IGMP Querier version to its default value.

Format	no set igmp querier version
Mode	Global Config

set igmp querier election participate

M4250

M4350

Use this command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is better (less) than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Default	disabled
Format	set igmp querier election participate <i>vlan-id</i>
Mode	VLAN Config (also referred to as VLAN Database)

no set igmp querier election participate

Use this command to set the Snooping Querier not to participate in querier election but go into non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

Format	no set igmp querier election participate <i>vlan-id</i>
Mode	VLAN Config (also referred to as VLAN Database)

show igmpsnooping querier

M4250

M4350

Use this command to display IGMP Snooping Querier information. Configured information is displayed whether or not IGMP Snooping Querier is enabled.

Format `show igmpsnooping querier [detail | vlan vlan-id]`

Mode Privileged EXEC

When the optional argument *vlan-id* is not used, the command displays the following information.

Field	Description
Admin Mode	Indicates whether or not IGMP Snooping Querier is active on the switch.
Admin Version	The version of IGMP that will be used while sending out the queries.
Querier Address	The IP Address which will be used in the IPv4 header while sending out IGMP queries. It can be configured using the appropriate command.
Query Interval	The amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
Querier Timeout	The amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for *vlan-id*, the following additional information displays.

Field	Description
VLAN Admin Mode	Indicates whether iGMP Snooping Querier is active on the VLAN.
VLAN Operational State	Indicates whether IGMP Snooping Querier is in "Querier" or "Non-Querier" state. When the switch is in Querier state, it will send out periodic general queries. When in Non-Querier state, it will wait for moving to Querier state and does not send out any queries.
VLAN Operational Max Response Time	Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.
Querier Election Participation	Indicates whether the IGMP Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	The IP address will be used in the IPv4 header while sending out IGMP queries on this VLAN. It can be configured using the appropriate command.
Operational Version	The version of IPv4 will be used while sending out IGMP queries on this VLAN.

Field	Description
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
Last Querier Version	Indicates the IGMP version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument **detail** is used, the command shows the global information and the information for all Querier-enabled VLANs.

set igmp proxy-querier

M4250

M4350

If a non-querier switch receives an IGMP leave message, the non-querier switch can send queries with 0::0 as source IP addresses. This command enables the switch to send such proxy queries through different command modes in the following ways:

- in Global Config mode, on the entire switch
- in Interface Config mode, on an interface
- in VLAN Config mode (also referred to as VLAN Database mode), on a particular VLAN and all interfaces participating in the VLAN.

By default, the proxy querier is enabled.

Default	enabled
Format	set igmp proxy-querier
Mode	Global Config Interface Config
Default	enabled
Format	set igmp proxy-querier vlan-id
Mode	VLAN Config (also referred to as VLAN Database)

no set igmp proxy-querier

This command stops the switch from sending proxy queries through different command modes in the following ways:

- in Global Config mode, on the entire switch
- in Interface Config mode, on an interface
- in VLAN Config mode (also referred to as VLAN Database mode), on a particular VLAN and all interfaces participating in the VLAN.

This command is specific to IGMP.

Format	<code>no set igmp proxy-querier</code>
Mode	Global Config Interface Config
Format	<code>no set igmp proxy-querier <i>vlan-id</i></code>
Mode	VLAN Config (also referred to as VLAN Database)

show igmpsnooping proxy-querier

M4250

M4350

This command shows the global admin mode of the IGMP snooping proxy-querier and the interface on which it is enabled.

Format	<code>show igmpsnooping proxy-querier</code>
Mode	Privileged EXEC

Command example:

```
(Netgear Switch) #show igmpsnooping proxy-querier
Admin Mode..... Enable
Interfaces Enabled for IGMP Proxy Querier..... 1/0/1
                                                1/0/2
                                                1/0/3
                                                1/0/4
```

MLD Snooping Commands

This section describes commands used for MLD Snooping. In IPv4, Layer 2 switches can use IGMP Snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded only to those interfaces associated with IP multicast addresses. In IPv6, MLD Snooping performs a similar function. With MLD Snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

Note: This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally, the switch gives precedence to the configured VLAN values over the configured interface values for most configurations when the interface participates in the VLAN.

set mld

M4250

M4350

This command enables MLD Snooping on the system (Global Config Mode) or an interface (Interface Config Mode). This command also enables MLD Snooping on a particular VLAN and enables MLD Snooping on all interfaces participating in a VLAN.

If an interface has MLD Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), MLD Snooping functionality is disabled on that interface. MLD Snooping functionality is re-enabled if you disable routing or remove port channel (LAG) membership from an interface that has MLD Snooping enabled.

MLD Snooping supports the following activities:

- Validation of address version, payload length consistencies and discarding of the frame upon error.
- Maintenance of the forwarding table entries based on the MAC address versus the IPv6 address.
- Filters out unknown IPv6 multicast packets on a VLAN if MLD snooping is enabled, with the exception of group addresses in the range ff2::/16 and FF05::X. These control packets are always flooded to all ports in the VLAN.

Format	set mld
Mode	Global Config Interface Config
Default	Enabled for VLAN 1; Disabled for other VLANs.
Format	set mld <i>vlan-id</i>
Mode	VLAN Mode

no set mld

Use this command to disable MLD Snooping on the system.

Format	no set mld
Mode	Global Config Interface Config
Format	no set mld <i>vlan-id</i>
Mode	VLAN Mode

set mld interfacemode

M4250

M4350

Use this command to enable MLD Snooping on all interfaces. If an interface has MLD Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), MLD Snooping functionality is disabled on that interface. MLD Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has MLD Snooping enabled.

Default	Disabled
Format	set mld interfacemode
Mode	Global Config

no set mld interfacemode

Use this command to disable MLD Snooping on all interfaces.

Format	no set mld interfacemode
Mode	Global Config

set mld fast-leave

M4250

M4350

Use this command to enable MLD Snooping fast-leave admin mode on a selected interface or VLAN. Enabling fast-leave allows the switch to immediately remove the Layer 2 LAN interface from its forwarding table entry upon receiving and MLD done message for that multicast group without first sending out MAC-based general queries to the interface.

Note: Enable fast-leave admin mode only on VLANs on which only one host is connected to each Layer 2 LAN port. This prevents the inadvertent dropping of other hosts that are connected to the same layer 2 LAN port but are still interested in receiving multicast traffic directed to that group.

Note: Fast-leave processing is supported only with MLD version 1 hosts.

Format	<code>set mld fast-leave</code>

Mode	Interface Config

Default	Enabled for VLAN 1; Disabled for other VLANs.

Format	<code>set mld fast-leave <i>vlan-id</i></code>

Mode	VLAN Mode

`no set mld fast-leave`

Use this command to disable MLD Snooping fast-leave admin mode on a selected interface or VLAN.

Format	<code>no set mld fast-leave</code>

Mode	Interface Config

Format	<code>no set mld fast-leave <i>vlan-id</i></code>

Mode	VLAN Mode

`set mld groupmembership-interval`

M4250

M4350

Use this command to set the MLD Group Membership Interval time on a VLAN, one interface or all interfaces. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the MLDv2 maximum response time value. The range is 2 to 3600 seconds.

Default	260 seconds
Format	<code>set mld groupmembership-interval seconds</code>
Mode	Interface Config Global Config
Default	260 seconds
Format	<code>set mld groupmembership-interval vlan-id seconds</code>
Mode	VLAN Mode

`no set groupmembership-interval`

Use this command to set the MLDv2 group membership Interval time to the default value.

Format	<code>no set mld groupmembership-interval</code>
Mode	Interface Config Global Config
Format	<code>no set mld groupmembership-interval vlan-id</code>
Mode	VLAN Mode

`set mld maxresponse`

M4250

M4350

Use this command to set the MLD maximum response time for the system, on a particular interface or VLAN. The maximum response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the MLD query interval time value. The range is 1 to 65 seconds.

Default	10 seconds
Format	<code>set mld maxresponse seconds</code>
Mode	Global Config Interface Config
Default	10 seconds
Format	<code>set mld maxresponse vlan-id seconds</code>
Mode	VLAN Mode

no set mld maxresponse

Use this command to set the max response time (on the interface or VLAN) to the default value.

Format	no set mld maxresponse
Mode	Global Config Interface Config
Format	no set mld maxresponse <i>vlan-id</i>
Mode	VLAN Mode

set mld mcrtreptime

M4250

M4350

Use this command to set the multicast router present expiration time. The time is set for the system, on a particular interface or VLAN. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite time-out, that is, no expiration.

Default	0
Format	set mld mcrtreptime <i>seconds</i>
Mode	Global Config Interface Config
Default	0
Format	set mld mcrtreptime <i>vlan-id seconds</i>
Mode	VLAN Config (also referred to as VLAN Database)

no set mld mcrtreptime

Use this command to set the multicast router present expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

Format	no set mld mcrtreptime
Mode	Global Config Interface Config
Format	no set mld mcrtreptime <i>vlan-id</i>
Mode	VLAN Config (also referred to as VLAN Database)

set mld mrouter

M4250

M4350

Use this command to configure the VLAN ID for the VLAN that has the multicast router attached mode enabled.

Format	<code>set mld mrouter <i>vlan-id</i></code>

Mode	Interface Config

no set mld mrouter

Use this command to disable multicast router attached mode for a VLAN with a particular VLAN ID.

Format	<code>no set mld mrouter <i>vlan-id</i></code>

Mode	Interface Config

set mld mrouter interface

M4250

M4350

Use this command to configure the interface as a multicast router-attached interface. When configured as a multicast router interface, the interface is treated as a multicast router-attached interface in all VLANs.

Default	disabled

Format	<code>set mld mrouter interface</code>

Mode	Interface Config

no set mld mrouter interface

Use this command to disable the status of the interface as a statically configured multicast router-attached interface.

Format	<code>no set mld mrouter interface</code>

Mode	Interface Config

set mld exclude-mrouter-intf

M4250

M4350

Use this command to control whether unknown multicast data is sent to an mrouter interface.

If either IGMP Snooping or MLD Snooping is enabled on a VLAN, by default, dynamic mrouter mode is enabled on the interface that receives MLD PDUs from the upstream router. When the mrouter mode is enabled on the interface, unknown multicast data is sent to that interface.

If you enter the command, the switch blocks all unknown multicast data through the mrouter port, whether the port is configured dynamically or statically. Only MLD PDUs are allowed to pass through the mrouter port to the upstream router interface.

Enter the command in Global Config mode to globally apply the setting to all interfaces.

Enter the command in VLAN Config mode (also referred to as VLAN Database mode) to apply the setting at VLAN or interface level.

For the VLAN configuration to take effect, you must first enter the **set mld exclude-mrouter-intf** command and then enter the same command for a specific VLAN.

Default	Enabled
Format	set mld exclude-mrouter-intf
Mode	Global Config
Default	Enabled
Format	set mld exclude-mrouter-intf <i>vlan-id</i>
Mode	VLAN Config (also referred to as VLAN Database)

no set mld exclude-mrouter-intf

Use this command to let the switch pass unknown multicast data to an mrouter interface.

Enter the command in Global Config mode to globally apply the setting to all interfaces.

Enter the command in VLAN Config mode (also referred to as VLAN Database mode) to apply the setting at VLAN or interface level.

Format	no set mld exclude-mrouter-intf
Mode	Global Config

Format	<code>no set mld exclude-mrouter-intf <i>vlan-id</i></code>

Mode	Global Config VLAN Config (also referred to as VLAN Database)

set mld-plus (Global Config)

M4250

M4350

This command enables both of the following global MLD Snooping configuration commands:

- **set mld**
- **set mld exclude-mrouter-intf**

Default	Enabled

Format	<code>set mld-plus</code>

Mode	Global Config

no set mld-plus (Global Config)

This command disables both of the following global MLD Snooping configuration commands:

- **set mld**
- **set mld exclude-mrouter-intf**

Format	<code>no set mld-plus</code>

Mode	Global Config

set mld-plus (VLAN Config)

M4250

M4350

After you enable the **set mld-plus** command, you can enable the **set mld-plus *vlan-id*** command to enable all of the following global MLD Snooping configuration commands at the VLAN level for a particular VLAN:

- **set mld *vlan-id***
- **set mld exclude-mrouter-intf *vlan-id***
- **set mld fast-leave *vlan-id***

The *vlan-id* argument in the **set mld-plus** *vlan-id* command can be a VLAN from 1 to 4093.

Default	Enabled for VLAN 1
Format	<code>set mld-plus <i>vlan-id</i></code>
Mode	VLAN Config (also referred to as VLAN Database)

`no set mld-plus (VLAN Config)`

This command disables all of the following global MLD Snooping configuration commands at the VLAN level for a particular VLAN:

- **set mld** *vlan-id*
- **set mld exclude-mrouter-intf** *vlan-id*
- **set mld fast-leave** *vlan-id*

The *vlan-id* argument in the **no set mld-plus** *vlan-id* command can be a VLAN from 1 to 4093.

Format	<code>no set mld-plus <i>vlan-id</i></code>
Mode	VLAN Config (also referred to as VLAN Database)

show mldsnooping

M4250

M4350

Use this command to display MLD Snooping information. Configured information is displayed whether or not MLD Snooping is enabled. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show igmpsnooping mrouter interface {<i>unit/slot/port</i> all}</code>
Mode	Privileged EXEC
Format	<code>show mldsnooping [<i>unit/slot/port</i> <i>vlan-id</i>]</code>
Mode	Privileged EXEC

When the optional arguments *unit/slot/port* or *vlan-id* are not used, the command displays the following information.

Term	Definition
Admin Mode	Indicates whether or not MLD Snooping is active on the switch.
Interfaces Enabled for MLD Snooping	Interfaces on which MLD Snooping is enabled.
MLD Control Frame Count	Displays the number of MLD Control frames that are processed by the CPU.
VLANs Enabled for MLD Snooping	VLANs on which MLD Snooping is enabled.
Exclude Mrouter Interface Mode	Indicates whether the Exclude Mrouter Interface is globally enabled or not.
MLD-Plus	Indicates whether MLD Plus is enabled or not.

When you specify the *unit/slot/port* values, the following information displays for the interface.

Term	Definition
Admin Mode	Indicates whether MLD Snooping is active on the interface.
Fast Leave Mode	Indicates whether MLD Snooping Fast Leave is active on the interface.
Group Membership Interval	Shows the period in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry. This value may be configured.
Max Response Time	Displays the period the switch waits after it sends a query on an interface because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time	Displays the period to wait before removing an interface from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

When you specify a value for *vlan-id*, the following information displays for the VLAN.

Term	Definition
Admin Mode	Indicates whether MLD Snooping is active on the VLAN.
Fast Leave Mode	Indicates whether MLD Snooping Fast Leave is active on the VLAN.
Group Membership Interval	Shows the period in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry. This value may be configured.
Max Response Time	Displays the period the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.

Term	Definition
Multicast Router Present Expiration Time	Displays the period to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.
Multicast Router Expiry Time	Indicates whether the Exclude Mrouter Interface is enabled or not.
MLD-Plus	Indicates whether MLD Plus is enabled or not.

show mldsnooping mrouter interface

M4250

M4350

Use this command to display information about statically configured multicast router attached interfaces. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show mldsnooping mrouter interface {unit/slot/port all}</code>

Mode	Privileged EXEC

Term	Definition
Interface	Shows the interface on which multicast router information is displayed.
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.
VLAN ID	Displays the list of VLANs of which the interface is a member.

show mldsnooping mrouter vlan

M4250

M4350

This command displays interfaces on which multicast routers are detected. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show mldsnooping mrouter vlan {vlan-id interface unit/slot/port}</code>

Mode	Privileged EXEC

Term	Definition
Interface	Shows the interface on which multicast router information is displayed.
VLAN ID	Displays the list of VLANs of which the interface is a member.

show mldsnoping ssm entries

M4250

M4350

Use this command to display the source specific multicast forwarding database built by MLD snooping.

A source, group, and VLAN combination can have few interfaces in “Include” mode and few interfaces in “Exclude” mode. In such instances, two rows for the same source, group, and VLAN combination are displayed.

Format	<code>show mldsnoping ssm entries</code>
Mode	Privileged EXEC

Term	Definition
VLAN	The VLAN on which the entry is learned.
Group	The IPv6 multicast group address.
Source	The IPv6 source address.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group.
Interfaces	- If Source Filter Mode is “Include,” specifies the list of interfaces on which a incoming packet is forwarded. If it’s source IP address is equal to the current entry’s Source, the destination IP address is equal to the current entry’s Group and the VLAN ID on which it arrived is current entry’s VLAN. - If Source Filter Mode is “Exclude,” specifies the list of interfaces on which a incoming packet is forwarded. If it’s source IP address is *not* equal to the current entry’s Source, the destination IP address is equal to current entry’s Group and VLAN ID on which it arrived is current entry’s VLAN.

show mldsnoping ssm stats

M4250

M4350

Use this command to display the statistics of MLD snooping’s SSMFDB.

Format	<code>show mldsnoping ssm stats</code>
Mode	Privileged EXEC

Term	Definition
Total Entries	The total number of entries that can possibly be in the MLD snooping's SSMFDB.
Most SSMFDB Entries Ever Used	The largest number of entries that have been present in the MLD snooping's SSMFDB.
Current Entries	The current number of entries in the MLD snooping's SSMFDB.

show mld Snooping ssm groups

M4250

M4350

Use this command to display the MLD SSM group membership information.

Format	show mld Snooping ssm groups
Mode	Privileged EXEC

Term	Definition
VLAN	VLAN on which the MLD v2 report is received.
Group	The IPv6 multicast group address.
Interface	The interface on which the MLD v2 report is received.
Reporter	The IPv6 address of the host that sent the MLDv2 report.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group.
Source Address List	List of source IP addresses for which source filtering is requested.

show mac-address-table mld Snooping

M4250

M4350

Use this command to display the MLD Snooping entries in the Multicast Forwarding Database (MFDB) table.

Format	show mac-address-table mld Snooping
Mode	Privileged EXEC

Term	Definition
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.

Term	Definition
Type	The type of entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol.)
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

clear mld Snooping

M4250

M4350

Use this command to delete all MLD snooping entries from the MFDB table.

Format	<code>clear mld Snooping</code>
Mode	Privileged EXEC

MLD Snooping Querier Commands

In an IPv6 environment, MLD 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 MLD Querier. The MLD query responses, known as MLD 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 will stop forwarding multicasts to the port where the end device is located.

This section describes the commands you use to configure and display information on MLD Snooping queries on the network and, separately, on VLANs.

Note: This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally, the switch gives precedence to the configured VLAN values over the configured interface values for most configurations when the interface participates in the VLAN.

set mld querier

M4250

M4350

Use this command to enable MLD Snooping Querier on the system (Global Config Mode) or on a VLAN. Using this command, you can specify the IP address that the snooping querier switch should use as a source address while generating periodic queries.

If a VLAN has MLD Snooping Querier enabled and MLD Snooping is operationally disabled on it, MLD Snooping Querier functionality is disabled on that VLAN. MLD Snooping functionality is re-enabled if MLD Snooping is operational on the VLAN.

The MLD Snooping Querier sends periodic general queries on the VLAN to solicit membership reports.

Default	disabled
Format	<code>set mld querier [address <i>ipv6-address</i>]</code>
Mode	Global Config
Default	disabled
Format	<code>set mld querier <i>vlan-id</i> [address <i>ipv6-address</i>]</code>
Mode	VLAN Mode

`no set mld querier`

Use this command to disable MLD Snooping Querier on the system. Use the optional parameter **address** to reset the querier address.

Format	<code>no set mld querier [address]</code>
Mode	Global Config
Format	<code>no set mld querier <i>vlan-id</i> [address]</code>
Mode	VLAN Mode

`set mld querier query-interval`

M4250

M4350

Use this command to set the MLD querier query interval time. It is the time in seconds, from 1–1800 seconds, that the switch waits before sending another general query.

Default	disabled
Format	<code>set mld querier query-interval <i>seconds</i></code>
Mode	Global Config

no set mld querier query-interval

Use this command to set the MLD Querier Query Interval time to its default value.

Format	no set mld querier query-interval

Mode	Global Config

set mld querier timer expiry

M4250

M4350

Use this command to set the MLD querier timer expiration period. It is the period in seconds, from 60–300 seconds, that the switch remains in non-querier mode after it has discovered a multicast querier in the network.

Default	60 seconds

Format	set mld querier timer expiry <i>seconds</i>

Mode	Global Config

no set mld querier timer expiry

Use this command to set the MLD querier timer expiration period to its default value.

Format	no set mld querier timer expiry

Mode	Global Config

set mld querier election participate

M4250

M4350

Use this command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is better (less) than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Default	disabled

Format	set mld querier election participate <i>vlan-id</i>

Mode	VLAN Config (also referred to as VLAN Database)

no set mld querier election participate

Use this command to set the snooping querier not to participate in querier election but go into a non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

Format	no set mld querier election participate <i>vlan-id</i>

Mode	VLAN Config (also referred to as VLAN Database)

show mld Snooping querier

M4250

M4350

Use this command to display MLD Snooping Querier information. Configured information is displayed whether or not MLD Snooping Querier is enabled.

Format	show mld Snooping querier [detail <i>vlan</i> <i>vlan-id</i>]

Mode	Privileged EXEC

If you do not specify a value for *vlan-id*, the command displays the following information.

Field	Description
Admin Mode	Indicates whether or not MLD Snooping Querier is active on the switch.
Admin Version	Indicates the version of MLD that will be used while sending out the queries. This is defaulted to MLD v1 and it cannot be changed.
Querier Address	Shows the IP address which will be used in the IPv6 header while sending out MLD queries. It can be configured using the appropriate command.
Query Interval	Shows the amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
Querier Timeout	Displays the amount of time to wait in the Non-Querier operational state before moving to a Querier state.

If you specify a value for *vlan-id*, the following information displays.

Field	Description
VLAN Admin Mode	Indicates whether MLD Snooping Querier is active on the VLAN.
VLAN Operational State	Indicates whether MLD Snooping Querier is in "Querier" or "Non-Querier" state. When the switch is in Querier state, it will send out periodic general queries. When in Non-Querier state, it will wait for moving to Querier state and does not send out any queries.
VLAN Operational Max Response Time	Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.

Field	Description
Querier Election Participate	Indicates whether the MLD Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	The IP address will be used in the IPv6 header while sending out MLD queries on this VLAN. It can be configured using the appropriate command.
Operational Version	This version of IPv6 will be used while sending out MLD queriers on this VLAN.
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
Last Querier Version	Indicates the MLD version of the most recent Querier from which a Query was received on this VLAN.

When the optional **detail** keyword is used, the command shows the global information and the information for all Querier-enabled VLANs.

set mld proxy-querier

M4250

M4350

If a non-querier switch receives an MLD leave message, the non-querier switch can send queries with 0::0 as the source IP addresses. This command enables the switch to send such proxy queries through different command modes the following ways:

- in Global Config mode, on the entire switch
- in Interface Config mode, on an interface
- in VLAN Config mode (also referred to as VLAN Database mode), on a particular VLAN and all interfaces participating in the VLAN.

By default, the proxy-querier is enabled.

Default	enabled
Format	<code>set mld proxy-querier</code>
Mode	Global Config Interface Config
Default	enabled
Format	<code>set mld proxy-querier vlan-id</code>
Mode	VLAN Config (also referred to as VLAN Database)

no set mld proxy-querier

This command stops the switch from sending proxy queries through different command modes in the following ways:

- in Global Config mode, on the entire switch
- in Interface Config mode, on an interface
- in VLAN Config mode (also referred to as VLAN Database mode), on a particular VLAN and all interfaces participating in the VLAN.

This command is specific to MLD.

Format	no set mld proxy-querier
Mode	Global Config Interface Config

Format	no set mld proxy-querier vlan-id
Mode	VLAN Config (also referred to as VLAN Database)

show mldsnopping proxy-querier

M4250

M4350

This command shows the global admin mode of the MLD snooping proxy-querier and the interface on which it is enabled.

Format	show mldsnopping proxy-querier
Mode	Privileged EXEC

Command example:

```
(Netgear Switch) #show mldsnopping proxy-querier
Admin Mode..... Enable
Interfaces Enabled for MLD Proxy Querier..... 1/0/1
                                                1/0/2
                                                1/0/3
```

Port Security Commands

This section describes the command you use to configure Port Security on the switch. Port security, which is also known as port MAC locking, allows you to secure the network by locking allowable MAC addresses on a port. Packets with a matching source MAC address are forwarded normally, and all other packets are discarded.

Note: To enable the SNMP trap specific to port security, see [snmp-server enable traps violation](#) on page 169.

port-security

M4250

M4350

This command enables port locking on an interface, a range of interfaces, or at the system level.

Default	disabled
Format	port-security
Mode	Global Config (to enable port locking globally) Interface Config (to enable port locking on an interface or range of interfaces)

no port-security

This command disables port locking for one (Interface Config) or all (Global Config) ports.

Format	no port-security
Mode	Global Config Interface Config

port-security aging time

M4250

M4350

Use this command to configure the aging time that defines the inactive duration of the dynamically-locked MAC addresses on an interface. The aging time is in minutes; the range is from 0 to 1440; The default is 5 minutes. An aging time of 0 implies that aging is disabled.

Default	disabled
Format	port-security aging time <i>minutes</i>
Mode	Interface Config

no port-security aging time

This command resets the aging time that defines the inactive duration of the dynamically-locked MAC addresses on an interface. The default is 5 minutes.

Format	no port-security
Mode	Interface Config

port-security max-dynamic

M4250

M4350

This command sets the maximum number of dynamically locked MAC addresses allowed on a specific port. The valid range is 0–4096.

Default	4096
Format	port-security max-dynamic <i>maxvalue</i>
Mode	Interface Config

no port-security max-dynamic

This command resets the maximum number of dynamically locked MAC addresses allowed on a specific port to its default value.

Format	no port-security max-dynamic
Mode	Interface Config

port-security max-static

M4250

M4350

This command sets the maximum number of statically locked MAC addresses allowed on a port. The valid range is 0–48.

Default	1
Format	<code>port-security max-static maxvalue</code>
Mode	Interface Config

no port-security max-static

This command sets maximum number of statically locked MAC addresses to the default value.

Format	<code>no port-security max-static</code>
Mode	Interface Config

port-security mac-address

M4250

M4350

This command adds a MAC address to the list of statically locked MAC addresses for an interface or range of interfaces. The *vlan-id* is the VLAN ID.

Format	<code>port-security mac-address mac-address vlan-id</code>
Mode	Interface Config

no port-security mac-address

This command removes a MAC address from the list of statically locked MAC addresses.

Format	<code>no port-security mac-address mac-address vlan-id</code>
Mode	Interface Config

port-security mac-address move

M4250**M4350**

This command converts dynamically locked MAC addresses to statically locked addresses for an interface or range of interfaces.

Format	port-security mac-address move

Mode	Interface Config

port-security mac-address sticky

M4250**M4350**

This command enables sticky mode Port MAC Locking on a port. If accompanied by a MAC address and a VLAN id (for interface config mode only), it adds a sticky MAC address to the list of statically locked MAC addresses. These sticky addresses are converted back to dynamically locked addresses if sticky mode is disabled on the port. The *vlan-id* is the VLAN ID. The Global command applies the sticky mode to all valid interfaces (physical and LAG). There is no global sticky mode as such.

Sticky addresses that are dynamically learned display in the output of the show running-config command as `port-security mac-address sticky mac vlan-id` entries. This distinguishes them from static entries.

Format	port-security mac-address sticky

Mode	Global Config

Format	port-security mac-address sticky [<i>mac-address</i> <i>vlan-id</i>]

Mode	Interface Config

Command example:

```
(NETGEAR) (Config) # port-security mac-address sticky
(NETGEAR) (Interface) # port-security mac-address sticky
(NETGEAR) (Interface) # port-security mac-address sticky
00:00:00:00:00:01 2
```

no port-security mac-address sticky

Use this command to disable the sticky mode.

Format	no port-security mac-address sticky

Mode	Global Config

Format	<code>no port-security mac-address sticky [mac-address vlan-id]</code>

Mode	Interface Config

port-security violation shutdown

M4250

M4350

This command allows an interface to be diagnostically disabled when a violation occurs for port MAC locking.

Format	<code>port-security violation shutdown</code>

Mode	Interface Config

no port-security violation shutdown

This command prevents an interface from being diagnostically disabled when a violation occurs for port MAC locking.

Format	<code>no port-security violation shutdown</code>

Mode	Interface Config

mac-address-table limit

M4250

M4350

This command enables VLAN port security. VLAN MAC locking lets you secure the network by locking down allowable MAC addresses on a specific VLAN. Packets with a matching source MAC address can be forwarded normally. All other packets are discarded. VLAN MAC locking locks the dynamic MAC entries.

If both VLAN and port MAC locking are enabled, VLAN MAC locking is given precedence over port MAC locking.

Default	Disabled

Format	<code>mac-address-table limit [action shutdown] [notification trap] [maximum-num] [vlan vlan-id]</code>

Mode	Global Config

Parameter	Description
action shutdown	After the MAC limit is reached, the action shuts down the ports participating in the VLAN.
notification tra	Enables the snmp-server enable traps violation command on the ports participating in the VLAN. After the MAC limit is reached, a log message is generated with the violation MAC address details.
<i>maximum-num</i>	The maximum number of MAC addresses.
vlan <i>vlan-id</i>	VLAN on which the MAC limit is applied. (Packets on all other VLANs are discarded.)

Command example:

```
(NETGEAR Switch) (Config)#mac-address-table limit 3 vlan 10
```

Command example:

```
(NETGEAR Switch) (Config)#mac-address-table limit action shutdown notification trap 6
vlan 100
```

no mac-address-table limit

This command disables VLAN port security on the specified VLAN.

Format	no mac-address-table limit [action shutdown] [notification trap] [<i>maximum-num</i>] [vlan <i>vlan-id</i>]

Mode	Global Config

show port-security

M4250

M4350

This command displays the port-security settings for the port or ports. If you do not use a parameter, the command displays the Port Security Administrative mode. Use the optional parameters to display the settings on a specific interface or on all interfaces. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Instead of *unit/slot/port*, **lag** *lag-intf-num* can be used as an alternate way to specify the LAG interface, in which *lag-intf-num* is the LAG port number.

Format	show port-security [<i>unit/slot/port</i> lag <i>lag-intf-num</i> all]

Mode	Privileged EXEC

Term	Definition
Admin Mode	Port Locking mode for the entire system. This field displays if you do not supply any parameters.

For each interface, or for the interface you specify, the following information displays.

Term	Definition
Admin Mode	Port Locking mode for the Interface.
Dynamic Limit	Maximum dynamically allocated MAC Addresses.
Static Limit	Maximum statically allocated MAC Addresses.
Violation Trap Mode	Whether violation traps are enabled.
Sticky Mode	The administrative mode of the port security Sticky Mode feature on the interface.

Command example:

```
(NETGEAR Switch) #show port-security 0/1
```

Intf	Admin Mode	Dynamic Limit	Static Limit	Violation Trap Mode	Sticky Mode
-----	-----	-----	-----	-----	-----
0/1	Disabled	1	1	Disabled	Enabled

show port-security dynamic

M4250

M4350

This command displays the dynamically locked MAC addresses for the port. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Instead of *unit/slot/port*, **lag** *lag-intf-num* can be used as an alternate way to specify the LAG interface, in which *lag-intf-num* is the LAG port number.

Format `show port-security dynamic {unit/slot/port | lag lag-intf-num}`

Mode Privileged EXEC

Term	Definition
MAC Address	MAC Address of dynamically locked MAC.

show port-security static

M4250

M4350

This command displays the statically locked MAC addresses for a port. This command displays the dynamically locked MAC addresses for the port. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Instead of *unit/slot/port*, **lag** *lag-intf-num* can be used as an alternate way to specify the LAG interface, in which *lag-intf-num* is the LAG port number.

Format	show port-security static {unit/slot/port lag lag-intf-num}	
Mode	Privileged EXEC	
Term	Definition	
Statically Configured MAC Address	The statically configured MAC address.	
VLAN ID	The ID of the VLAN that includes the host with the specified MAC address.	
Sticky	Indicates whether the static MAC address entry is added in sticky mode.	

Command example:

```
(NETGEAR Switch) #show port-security static 1/0/1
Number of static MAC addresses configured: 2
Statically configured MAC Address      VLAN ID      Sticky
-----
00:00:00:00:00:01                     2             Yes
00:00:00:00:00:02                     2             No
```

show port-security violation

M4250

M4350

This command displays the source MAC address of the last packet discarded on a locked port. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Instead of *unit/slot/port*, **lag** *lag-intf-num* can be used as an alternate way to specify the LAG interface, in which *lag-intf-num* is the LAG port number.

Format	<code>show port-security violation {unit/slot/port lag lag-intf-num}</code>
Mode	Privileged EXEC
Term	Definition
MAC Address	The source MAC address of the last frame that was discarded at a locked port.
VLAN ID	The VLAN ID, if applicable, associated with the MAC address of the last frame that was discarded at a locked port.

LLDP (802.1AB) Commands

This section describes the command you use to configure Link Layer Discovery Protocol (LLDP), which is defined in the IEEE 802.1AB specification. LLDP allows stations on an 802 LAN to advertise major capabilities and physical descriptions. The advertisements allow a network management system (NMS) to access and display this information.

`lldp transmit`

M4250

M4350

Use this command to enable the LLDP advertise capability on an interface or a range of interfaces.

Default	disabled
Format	<code>lldp transmit</code>
Mode	Interface Config

`no lldp transmit`

Use this command to return the local data transmission capability to the default.

Format	<code>no lldp transmit</code>
Mode	Interface Config

lldp receive

M4250**M4350**

Use this command to enable the LLDP receive capability on an interface or a range of interfaces.

Default	disabled
Format	lldp receive
Mode	Interface Config

no lldp receive

Use this command to return the reception of LLDPDUs to the default value.

Format	no lldp receive
Mode	Interface Config

lldp timers

M4250**M4350**

Use this command to set the timing parameters for local data transmission on ports enabled for LLDP. The *interval-seconds* determines the number of seconds to wait between transmitting local data LLDPDUs. The range is 5–32768 seconds. The *hold-value* is the multiplier on the transmit interval that sets the TTL in local data LLDPDUs. The multiplier range is 2–10. The *reinit-seconds* is the delay before reinitialization, and the range is 1–0 seconds.

Default	interval—30 seconds hold—4 reinit—2 seconds
Format	lldp timers [interval <i>interval-seconds</i>] [hold <i>hold-value</i>] [reinit <i>reinit-seconds</i>]
Mode	Global Config

no lldp timers

Use this command to return any or all timing parameters for local data transmission on ports enabled for LLDP to the default values.

Format	no lldp timers [interval] [hold] [reinit]
Mode	Global Config

lldp transmit-tlv

M4250**M4350**

Use this command to specify which optional type length values (TLVs) in the 802.1AB basic management set are transmitted in the LLDPDUs from an interface or range of interfaces. Use *sys-name* to transmit the system name TLV.

To configure the system name, see [snmp-server](#) on page 162. Use **sys-desc** to transmit the system description TLV. Use **sys-cap** to transmit the system capabilities TLV. Use **port-desc** to transmit the port description TLV. To configure the port description, see [description \(Interface Config\)](#) on page 483.

Default	no optional TLVs are included
Format	lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]
Mode	Interface Config

no lldp transmit-tlv

Use this command to remove an optional TLV from the LLDPDUs. Use the command without parameters to remove all optional TLVs from the LLDPDU.

Format	no lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]
Mode	Interface Config

lldp transmit-tlv vlan

M4250**M4350**

Use this command to specify if the LLDP Port VLAN (PVID) TLV or LLDP VLAN Name TLV are transmitted in the LLDPDUs from an interface or range of interfaces.

Default	no optional TLVs are included
Format	lldp transmit-tlv vlan {port-vlan vlan-name}
Mode	Interface Config

no lldp transmit-tlv vlan

Use this command to remove the LLDP Port VLAN (PVID) TLV or LLDP VLAN Name TLV from the LLDPDUs.

Format	no lldp transmit-tlv vlan {port-vlan vlan-name}
Mode	Interface Config

lldp transmit-tlv link-aggregation

M4250**M4350**

Use this command to specify if the Link Aggregation TLV is transmitted in the LLDPDUs from an interface or range of interfaces.

Default	no optional TLVs are included
Format	lldp transmit-tlv link-aggregation
Mode	Interface Config

no lldp transmit-tlv link-aggregation

Use this command to remove the Link Aggregation TLV from the LLDPDUs.

Format	no lldp transmit-tlv link-aggregation
Mode	Interface Config

lldp transmit-tlv max-frame-size

M4250**M4350**

Use this command to specify if the Maximum Frame Size TLV is transmitted in the LLDPDUs from an interface or range of interfaces.

Default	no optional TLVs are included
Format	lldp transmit-tlv vmax-frame-size
Mode	Interface Config

no lldp transmit-tlv max-frame-size

Use this command to remove the Maximum Frame Size TLV from the LLDPDUs.

Format	no lldp transmit-tlv max-frame-size
Mode	Interface Config

lldp transmit-mgmt

M4250

M4350

Use this command to include transmission of the local system management address information in the LLDPDUs. This command can be used to configure a single interface or a range of interfaces.

Format	lldp transmit-mgmt

Mode	Interface Config

no lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. Use this command to cancel inclusion of the management information in LLDPDUs.

Format	no lldp transmit-mgmt

Mode	Interface Config

lldp notification

M4250

M4350

Use this command to enable remote data change notifications on an interface or a range of interfaces.

Default	disabled

Format	lldp notification

Mode	Interface Config

no lldp notification

Use this command to disable notifications.

Default	disabled

Format	no lldp notification

Mode	Interface Config

lldp notification-interval

M4250**M4350**

Use this command to configure how frequently the system sends remote data change notifications. The *interval* parameter is the number of seconds to wait between sending notifications. The valid interval range is 5–3600 seconds.

Default	5
Format	lldp notification-interval <i>interval</i>
Mode	Global Config

no lldp notification-interval

Use this command to return the notification interval to the default value.

Format	no lldp notification-interval
Mode	Global Config

lldp portid-subtype

M4250**M4350**

Use this command to set the LLDP port ID subtype for the **show lldp local-device detail** command as an interface name (use the **interface-name** keyword) or a MAC address (use the **mac-address** keyword).

Default	mac-address
Format	lldp portid-subtype [interface-name mac-address]
Mode	Interface Config

no lldp portid-subtype

Use this command to reset the LLDP port ID subtype for the **show lldp local-device detail** command to the default (the **mac-address** keyword).

Format	no lldp portid-subtype
Mode	Interface Config

clear lldp statistics

M4250**M4350**

Use this command to reset all LLDP statistics, including MED-related information.

Format	<code>clear lldp statistics</code>

Mode	Privileged Exec

clear lldp remote-data

M4250**M4350**

Use this command to delete all information from the LLDP remote data table, including MED-related information.

Format	<code>clear lldp remote-data</code>

Mode	Privileged Exec

show lldp

M4250**M4350**

Use this command to display a summary of the current LLDP configuration.

Format	<code>show lldp</code>

Mode	Privileged Exec

Term	Definition
Transmit Interval	How frequently the system transmits local data LLDPDUs, in seconds.
Transmit Hold Multiplier	The multiplier on the transmit interval that sets the TTL in local data LLDPDUs.
Re-initialization Delay	The delay before reinitialization, in seconds.
Notification Interval	How frequently the system sends remote data change notifications, in seconds.

show lldp interface

M4250**M4350**

Use this command to display a summary of the current LLDP configuration for a specific interface or for all interfaces. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	<code>show lldp interface {unit/slot/port all}</code>
Mode	Privileged Exec
Term	Definition
Interface	The interface in a <i>unit/slot/port</i> format.
Link	Shows whether the link is up or down.
Transmit	Shows whether the interface transmits LLDPDUs.
Receive	Shows whether the interface receives LLDPDUs.
Notify	Shows whether the interface sends remote data change notifications.
TLVs	Shows whether the interface sends optional TLVs in the LLDPDUs. The TLV codes can be 0 (Port Description), 1 (System Name), 2 (System Description), or 3 (System Capability).
Mgmt	Shows whether the interface transmits system management address information in the LLDPDUs.

show lldp statistics

M4250**M4350**

Use this command to display the current LLDP traffic and remote table statistics for a specific interface or for all interfaces. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	<code>show lldp statistics {unit/slot/port all}</code>
Mode	Privileged Exec

Term	Definition
Last Update	The amount of time since the last update to the remote table in days, hours, minutes, and seconds.
Total Inserts	Total number of inserts to the remote data table.
Total Deletes	Total number of deletes from the remote data table.
Total Drops	Total number of times the complete remote data received was not inserted due to insufficient resources.
Total Ageouts	Total number of times a complete remote data entry was deleted because the Time to Live interval expired.

The table contains the following column headings.

Term	Definition
Interface	The interface.
TX Total	Total number of LLDP packets transmitted on the port.
RX Total	Total number of LLDP packets received on the port.
Discards	Total number of LLDP frames discarded on the port for any reason.
Errors	The number of invalid LLDP frames received on the port.
Ageouts	Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.
TVL Discards	The number of TLVs discarded.
TVL Unknowns	Total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.
TLV MED	The total number of LLDP-MED TLVs received on the interface.
TLV 802.1	The total number of LLDP TLVs received on the interface which are of type 802.1.
TLV 802.3	The total number of LLDP TLVs received on the interface which are of type 802.3.

show lldp remote-device

M4250

M4350

Use this command to display summary information about remote devices that transmit current LLDP data to the system. You can show information about LLDP remote data received on all ports or on a specific port. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Fully Managed Switches M4250 and M4350 Series

Format `show lldp remote-device {unit/slot/port | all}`

Mode Privileged EXEC

Term	Definition
Local Interface	The interface that received the LLDPDU from the remote device.
RemID	An internal identifier to the switch to mark each remote device to the system.
Chassis ID	The ID that is sent by a remote device as part of the LLDP message, it is usually a MAC address of the device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.

Command example:

```
(NETGEAR switch) #show lldp remote-device all
```

LLDP Remote Device Summary

Local Interface	RemID	Chassis ID	Port ID	System Name
-----	-----	-----	-----	-----
0/1				
0/2				
0/3				
0/4				
0/5				
0/6				
0/7	2	00:FC:E3:90:01:0F	00:FC:E3:90:01:11	
0/7	3	00:FC:E3:90:01:0F	00:FC:E3:90:01:12	
0/7	4	00:FC:E3:90:01:0F	00:FC:E3:90:01:13	
0/7	5	00:FC:E3:90:01:0F	00:FC:E3:90:01:14	
0/7	1	00:FC:E3:90:01:0F	00:FC:E3:90:03:11	
0/7	6	00:FC:E3:90:01:0F	00:FC:E3:90:04:11	
0/8				
0/9				
0/10				
0/11				
0/12				

show lldp remote-device detail

M4250

M4350

Use this command to display detailed information about remote devices that transmit current LLDP data to an interface on the system. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format `show lldp remote-device detail unit/slot/port`

Mode Privileged EXEC

Term	Definition
Local Interface	The interface that received the LLDPDU from the remote device.
Remote Identifier	An internal identifier to the switch to mark each remote device to the system.
Chassis ID Subtype	The type of identification used in the Chassis ID field.
Chassis ID	The chassis of the remote device.
Port ID Subtype	The type of port on the remote device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.
System Description	Describes the remote system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format. The port description is configurable.
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	For each interface on the remote device with an LLDP agent, lists the type of address the remote LLDP agent uses and specifies the address used to obtain information related to the device.
Time To Live	The amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.

Command example:

```
(NETGEAR switch) #show lldp remote-device detail 0/7
```

```
LLDP Remote Device Detail
```

```
Local Interface: 0/7
```

```
Remote Identifier: 2
```

```
Chassis ID Subtype: MAC Address
```

```
Chassis ID: 00:FC:E3:90:01:0F
```

```
Port ID Subtype: MAC Address
```

```
Port ID: 00:FC:E3:90:01:11
```

```
System Name:
```

```
System Description:
```

```
Port Description:
```

```
System Capabilities Supported:
```

```
System Capabilities Enabled:
```

```
Time to Live: 24 seconds
```

show lldp local-device**M4250****M4350**

Use this command to display summary information about the advertised LLDP local data. This command can display summary information or detail for each interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	<code>show lldp local-device {unit/slot/port all}</code>
Mode	Privileged EXEC

Term	Definition
Interface	The interface in a <i>unit/slot/port</i> format.
Port ID	The port ID associated with this interface.
Port Description	The port description associated with the interface.

show lldp local-device detail

M4250

M4350

Use this command to display detailed information about the LLDP data a specific interface transmits. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format `show lldp local-device detail unit/slot/port`

Mode Privileged EXEC

Term	Definition
Interface	The interface that sends the LLDPDU.
Chassis ID Subtype	The type of identification used in the Chassis ID field.
Chassis ID	The chassis of the local device.
Port ID Subtype	The type of port on the local device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the local device.
System Description	Describes the local system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format.
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	The type of address and the specific address the local LLDP agent uses to send and receive information.

LLDP-MED Commands

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) (ANSI-TIA-1057) provides an extension to the LLDP standard. Specifically, LLDP-MED provides extensions for network configuration and policy, device location, Power over Ethernet (PoE) management and inventory management.

lldp med

M4250

M4350

Use this command to enable MED on an interface or a range of interfaces. By enabling MED, you will be effectively enabling the transmit and receive function of LLDP.

Default	disabled
Format	lldp med
Mode	Interface Config

no lldp med

Use this command to disable MED.

Format	no lldp med
Mode	Interface Config

lldp med confignotification

M4250

M4350

Use this command to configure an interface or a range of interfaces to send the topology change notification.

Default	disabled
Format	lldp med confignotification
Mode	Interface Config

no lldp med confignotification

Use this command to disable notifications.

Format	no lldp med confignotification

Mode	Interface Config

lldp med transmit-tlv

M4250

M4350

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set are transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs) from an interface or a range of interfaces.

Default	By default, the capabilities and network policy TLVs are included.

Format	lldp med transmit-tlv [capabilities] [inventory] [location] [network-policy] [ex-pd] [ex-pse]

Mode	Interface Config

Parameter	Definition
capabilities	Transmit the LLDP capabilities TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.
ex-pd	Transmit the LLDP extended PD TLV. This option is available only on a switch that can function as a Powered Device (PD).
ex-pse	Transmit the LLDP extended PSE TLV. (This option is available only on a switch that can function as Power Sourcing Equipment (PSE).

no lldp med transmit-tlv

Use this command to remove a TLV from an interface or a range of interfaces.

Format	no lldp med transmit-tlv [capabilities] [network-policy] [location] [inventory] [ex-pse] [ex-pd]

Mode	Interface Config

lldp med transmit-tlv all

M4250**M4350**

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set are globally transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default	By default, the capabilities and network policy TLVs are included.
Format	lldp med transmit-tlv all [capabilities] [inventory] [location] [network-policy] [ex-pd] [ex-pse]
Mode	Global Config
Term	Definition
capabilities	Transmit the LLDP capabilities TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.
ex-pd	Transmit the LLDP extended PD TLV. This option is available only on a switch that can function as a Powered Device (PD).
ex-pse	Transmit the LLDP extended PSE TLV. (This option is available only on a switch that can function as Power Sourcing Equipment (PSE).

no lldp med transmit-tlv

Use this command to globally remove a TLV.

Format	no lldp med transmit-tlv [capabilities] [network-policy] [location] [inventory] [ex-pse] [ex-pd]
Mode	Global Config

lldp med all

M4250**M4350**

Use this command to enable LLDP-MED on all ports.

Format	lldp med all
Mode	Global Config

no lldp med all

Use this command to disable LLDP-MED on all ports.

Format	no lldp med all

Mode	Global Config

lldp med confignotification all

M4250

M4350

Use this command to enable all ports to send topology change notifications.

Format	lldp med confignotification all

Mode	Global Config

no lldp med confignotification all

Use this command to prevent all ports from sending topology change notifications.

Format	no lldp med confignotification all

Mode	Global Config

lldp med faststartrepeatcount

M4250

M4350

Use this command to set the value of the fast start repeat count. The *count argument* is the number of LLDP PDUs that are transmitted. The range is 1 to 10.

Default	3

Format	lldp med faststartrepeatcount <i>count</i>

Mode	Global Config

no lldp med faststartrepeatcount

Use this command to return the value of the fast start repeat count to the default value.

Format	no lldp med faststartrepeatcount

Mode	Global Config

show lldp med

M4250**M4350**

Use this command to display a summary of the current LLDP MED configuration.

Format	show lldp med

Mode	Privileged Exec

Command example:

```
(NETGEAR Switch) #show lldp med
```

```
LLDP MED Global Configuration
```

```
Fast Start Repeat Count: 3
```

```
Device Class: Network Connectivity
```

```
(NETGEAR Switch) #
```

show lldp med interface

M4250**M4350**

Use this command to display a summary of the current LLDP MED configuration for a specific interface. The **all** keywords specifies all LLDP interfaces. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	show lldp med interface {unit/slot/port all}

Mode	Privileged Exec

Command example:

```
(NETGEAR Switch) #show lldp med interface all
```

Interface	Link	configMED	operMED	ConfigNotify	TLVsTx
-----	-----	-----	-----	-----	-----
1/0/1	Down	Disabled	Disabled	Disabled	0,1
1/0/2	Up	Disabled	Disabled	Disabled	0,1
1/0/3	Down	Disabled	Disabled	Disabled	0,1
1/0/4	Down	Disabled	Disabled	Disabled	0,1
1/0/5	Down	Disabled	Disabled	Disabled	0,1

Fully Managed Switches M4250 and M4350 Series

1/0/6	Down	Disabled	Disabled	Disabled	0,1
1/0/7	Down	Disabled	Disabled	Disabled	0,1
1/0/8	Down	Disabled	Disabled	Disabled	0,1
1/0/9	Down	Disabled	Disabled	Disabled	0,1
1/0/10	Down	Disabled	Disabled	Disabled	0,1
1/0/11	Down	Disabled	Disabled	Disabled	0,1
1/0/12	Down	Disabled	Disabled	Disabled	0,1
1/0/13	Down	Disabled	Disabled	Disabled	0,1
1/0/14	Down	Disabled	Disabled	Disabled	0,1

TLV Codes: 0- Capabilities, 1- Network Policy
 2- Location, 3- Extended PSE
 4- Extended Pd, 5- Inventory
--More-- or (q)uit

Command example:

(NETGEAR Switch) #show lldp med interface 1/0/2

Interface	Link	configMED	operMED	ConfigNotify	TLVsTx
1/0/2	Up	Disabled	Disabled	Disabled	0,1

TLV Codes: 0- Capabilities, 1- Network Policy
 2- Location, 3- Extended PSE
 4- Extended Pd, 5- Inventory

show lldp med local-device detail

M4250

M4350

Use this command to display detailed information about the LLDP MED data that a specific interface transmits. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	show lldp med local-device detail <i>unit/slot/port</i>

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show lldp med local-device detail 1/0/8
```

```
LLDP MED Local Device Detail
```

```
Interface: 1/0/8
```

```
Network Policies
```

```
Media Policy Application Type : voice
```

```
Vlan ID: 10
```

```
Priority: 5
```

```
DSCP: 1
```

```
Unknown: False
```

```
Tagged: True
```

```
Media Policy Application Type : streamingvideo
```

```
Vlan ID: 20
```

```
Priority: 1
```

```
DSCP: 2
```

```
Unknown: False
```

```
Tagged: True
```

```
Inventory
```

```
Hardware Rev: xxx xxx xxx
```

```
Firmware Rev: xxx xxx xxx
```

```
Software Rev: xxx xxx xxx
```

```
Serial Num: xxx xxx xxx
```

```
Mfg Name: xxx xxx xxx
```

```
Model Name: xxx xxx xxx
```

```
Asset ID: xxx xxx xxx
```

```
Location
```

```
Subtype: elin
```

```
Info: xxx xxx xxx
```

```
Extended POE
```

```
Device Type: pseDevice
```

```
Extended POE PSE
```

```
Available: 0.3 Watts
```

```
Source: primary
```

```
Priority: critical
```

```
Extended POE PD
```

```
Required: 0.2 Watts
```

Source: local

Priority: low

show lldp med remote-device

M4250**M4350**

Use this command to display the summary information about remote devices that transmit current LLDP MED data to the system. You can show information about LLDP MED remote data received on all LLDP interfaces or on a specific physical interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	show lldp med remote-device { <i>unit/slot/port</i> all}

Mode	Privileged EXEC

Term	Definition
Local Interface	The interface that received the LLDPDU from the remote device.
Remote ID	An internal identifier to the switch to mark each remote device to the system.
Device Class	Device classification of the remote device.

Command example:

```
(NETGEAR Switch) #show lldp med remote-device all
```

LLDP MED Remote Device Summary

```
Local
Interface Remote ID Device Class
-----
1/0/8      1      Class I
1/0/9      2      Not Defined
1/0/10     3      Class II
1/0/11     4      Class III
1/0/12     5      Network Con
```

show lldp med remote-device detail

M4250**M4350**

Use this command to display detailed information about remote devices that transmit current LLDP MED data to an interface on the system. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	show lldp med remote-device detail <i>unit/slot/port</i>
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show lldp med remote-device detail 1/0/8
```

```
LLDP MED Remote Device Detail
```

```
Local Interface: 1/0/8
```

```
Remote Identifier: 18
```

```
Capabilities
```

```
MED Capabilities Supported: capabilities, networkpolicy, location, extendedpse
```

```
MED Capabilities Enabled: capabilities, networkpolicy
```

```
Device Class: Endpoint Class I
```

```
Network Policies
```

```
Media Policy Application Type : voice
```

```
Vlan ID: 10
```

```
Priority: 5
```

```
DSCP: 1
```

```
Unknown: False
```

```
Tagged: True
```

```
Media Policy Application Type : streamingvideo
```

```
Vlan ID: 20
```

```
Priority: 1
```

```
DSCP: 2
```

```
Unknown: False
```

```
Tagged: True
```

```
Inventory
```

```
Hardware Rev: xxx xxx xxx
```


Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx

Location
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice

Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical

Extended POE PD

Required: 0.2 Watts
Source: local
Priority: low

Denial of Service Commands

This section describes the commands you use to configure Denial of Service (DoS) Control. The switch provides support for classifying and blocking specific types of Denial of Service attacks. You can configure your system to monitor and block these types of attacks:

- **SIP = DIP.** Source IP address = Destination IP address.
- **First Fragment.** TCP Header size smaller than configured value.
- **TCP Fragment.** Allows the device to drop packets that have a TCP payload where the IP payload length minus the IP header size is less than the minimum allowed TCP header size.
- **TCP Flag.** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **L4 Port.** Source TCP/UDP Port = Destination TCP/UDP Port.
- **ICMP.** Limiting the size of ICMP Ping packets.
- **SMAC = DMAC.** Source MAC address = Destination MAC address.

- **TCP Port.** Source TCP Port = Destination TCP Port.
- **UDP Port.** Source UDP Port = Destination UDP Port.
- **TCP Flag & Sequence.** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **TCP Offset.** Allows the device to drop packets that have a TCP header Offset set to 1.
- **TCP SYN.** TCP Flag SYN set.
- **TCP SYN & FIN.** TCP Flags SYN and FIN set.
- **TCP FIN & URG & PSH.** TCP Flags FIN and URG and PSH set and TCP Sequence Number = 0.
- **ICMP V6.** Limiting the size of ICMPv6 Ping packets.
- **ICMP Fragment.** Checks for fragmented ICMP packets.

dos-control all

M4250

M4350

This command enables Denial of Service protection checks globally.

Default	disabled
Format	dos-control all
Mode	Global Config

no dos-control all

This command disables Denial of Service prevention checks globally.

Format	no dos-control all
Mode	Global Config

dos-control sipdip

M4250

M4350

This command enables Source IP address = Destination IP address (SIP = DIP) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SIP = DIP, the packets are dropped if the mode is enabled.

Default	disabled

Format	<code>dos-control sipdip</code>

Mode	Global Config

`no dos-control sipdip`

This command disables Source IP address = Destination IP address (SIP = DIP) Denial of Service prevention.

Format	<code>no dos-control sipdip</code>

Mode	Global Config

`dos-control firstfrag`

M4250

M4350

This command enables Minimum TCP Header Size Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with a TCP Header Size smaller than the configured value, the packets are dropped if the mode is enabled. The default is disabled. The range is 0–255. If you enable the **`dos-control firstfrag`** command but do not provide a minimum TCP header size, the switch sets the value to 20.

Default	disabled (20)

Format	<code>dos-control firstfrag [size]</code>

Mode	Global Config

`no dos-control firstfrag`

This command sets Minimum TCP Header Size Denial of Service protection to the default value of disabled.

Format	<code>no dos-control firstfrag</code>

Mode	Global Config

`dos-control tcpfrag`

M4250

M4350

This command enables TCP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack and packets with a TCP payload

in which the IP payload length minus the IP header size is less than the minimum allowed TCP header size are dropped.

Default	disabled
Format	<code>dos-control tcpfrag</code>
Mode	Global Config

`no dos-control tcpfrag`

This command disables TCP Fragment Denial of Service protection.

Format	<code>no dos-control tcpfrag</code>
Mode	Global Config

`dos-control tcpflag`

M4250

M4350

This command enables TCP Flag Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attacks.

If the mode is enabled, packets that ingress with one of the following conditions are dropped:

- The TCP Flag SYN is set and the source port number is lower less 1024
- The TCP Control Flag is set to 0 and the TCP Sequence Number is set to 0
- The TCP Flags FIN, URG, and PSH are set and the TCP Sequence Number set to 0
- The TCP Flags SYN and FIN are both set

Default	disabled
Format	<code>dos-control tcpflag</code>
Mode	Global Config

`no dos-control tcpflag`

This command sets disables TCP Flag Denial of Service protections.

Format	<code>no dos-control tcpflag</code>
Mode	Global Config

`dos-control l4port`**M4250****M4350**

This command enables L4 Port Denial of Service protections. If the mode with a Source TCP/UDP Port Number equal to the Destination TCP/UDP Port Number, the packets are dropped if the mode is enabled.

Note: Some applications mirror source and destination L4 ports. For example, RIP uses 520 for both. If you enable the `dos-control l4port` command, applications such as RIP can experience packet loss which would render the application inoperable.

Default	Disabled
Format	<code>dos-control l4port</code>
Mode	Global Config

`no dos-control l4port`

This command disables L4 Port Denial of Service protections.

Format	<code>no dos-control l4port</code>
Mode	Global Config

`dos-control port-ddisable`**M4250****M4350**

This command moves an interface that is under DoS attack to the D-Disable state. In the D-Disable state, the interface is not able to receive or send data packets. To use the interface again, manually reenables the port or configure auto-recovery.

Default	Disabled
Format	<code>dos-control port-ddisable</code>
Mode	Global Config

no dos-control port-ddisable

This command moves an interface that is or was under DoS attack out of the D-Disable state.

Format	no dos-control port-ddisable
Mode	Global Config

dos-control smacdmac

M4250

M4350

This command enables Source MAC address = Destination MAC address (SMAC = DMAC) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SMAC = DMAC, the packets are dropped if the mode is enabled.

Default	disabled
Format	dos-control smacdmac
Mode	Global Config

no dos-control smacdmac

This command disables Source MAC address = Destination MAC address (SMAC = DMAC) DoS protection.

Format	no dos-control smacdmac
Mode	Global Config

dos-control tcpport

M4250

M4350

This command enables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source TCP Port = Destination TCP Port, the packets are dropped if the mode is enabled.

Default	Disabled
Format	dos-control tcpport
Mode	Global Config

no dos-control tcpport

This command disables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection.

Format	no dos-control tcpport

Mode	Global Config

dos-control udpport

M4250

M4350

This command enables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) DoS protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source UDP Port = Destination UDP Port, the packets are dropped if the mode is enabled.

Default	Disabled

Format	dos-control udpport

Mode	Global Config

no dos-control udpport

This command disables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) Denial of Service protection.

Format	no dos-control udpport

Mode	Global Config

dos-control tcpflagseq

M4250

M4350

This command enables TCP Flag and Sequence Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack.

If the mode is enabled, packets that ingress with one of the following conditions are dropped:

- The TCP Flag SYN is set and the source port number is lower than 1024
- The TCP Control Flag is set to 0 and the TCP Sequence Number is set to 0
- The TCP Flags FIN, URG, and PSH are set and the TCP Sequence Number is set to 0
- The TCP Flags SYN and FIN are both set

Default	Disabled
Format	<code>dos-control tcpflagseq</code>
Mode	Global Config

`no dos-control tcpflagseq`

This command sets disables TCP Flag and Sequence Denial of Service protection.

Format	<code>no dos-control tcpflagseq</code>
Mode	Global Config

`dos-control tcpoffset`

M4250

M4350

This command enables TCP Offset Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with the TCP Header Offset set equal to one (1), the packets are dropped if the mode is enabled.

Default	Disabled
Format	<code>dos-control tcpoffset</code>
Mode	Global Config

`no dos-control tcpoffset`

This command disabled TCP Offset Denial of Service protection.

Format	<code>no dos-control tcpoffset</code>
Mode	Global Config

`dos-control tcpsyn`

M4250

M4350

This command enables TCP SYN and L4 source = 0-1023 Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with the TCP flag SYN set and an L4 source port from 0 to 1023, the packets are dropped if the mode is enabled.

Default	Disabled

Format	<code>dos-control tcpsyn</code>

Mode	Global Config

```
no dos-control tcpsyn
```

This command sets disables TCP SYN and L4 source = 0-1023 Denial of Service protection.

Format	<code>no dos-control tcpsyn</code>

Mode	Global Config

```
dos-control tcpsynfin
```

M4250

M4350

This command enables TCP SYN and FIN Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with the TCP flags SYN and FIN set, the packets are dropped if the mode is enabled.

Default	Disabled

Format	<code>dos-control tcpsynfin</code>

Mode	Global Config

```
no dos-control tcpsynfin
```

This command sets disables TCP SYN & FIN Denial of Service protection.

Format	<code>no dos-control tcpsynfin</code>

Mode	Global Config

```
dos-control tcpfinurgpsh
```

M4250

M4350

This command enables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with the TCP FIN, URG, and PSH flags set and the TCP Sequence Number set to 0, the packets are dropped if the mode is enabled.

Default	Disabled
Format	<code>dos-control tcpfinurgpsh</code>
Mode	Global Config

```
no dos-control tcpfinurgpsh
```

This command sets disables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections.

Format	<code>no dos-control tcpfinurgpsh</code>
Mode	Global Config

```
dos-control icmpv4
```

M4250

M4350

This command enables Maximum ICMPv4 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv4 Echo Request (PING) packets ingress with a size greater than the configured value, the packets are dropped if the mode is enabled. The value for the size is from 0–16376.

Default	Disabled (512)
Format	<code>dos-control icmpv4 [size]</code>
Mode	Global Config

```
no dos-control icmpv4
```

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	<code>no dos-control icmpv4</code>
Mode	Global Config

```
dos-control icmpv6
```

M4250

M4350

This command enables Maximum ICMPv6 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv6 Echo Request (PING) packets ingress with a size greater than the configured value, the packets are dropped if the mode is enabled. The value for the size is from 0–16376.

Default	Disabled (512)

Format	<code>dos-control icmpv6 [size]</code>

Mode	Global Config

`no dos-control icmpv6`

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	<code>no dos-control icmpv6</code>

Mode	Global Config

`dos-control icmpfrag`

M4250

M4350

This command enables ICMP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If fragmented ICMP packets ingress, the packets are dropped if the mode is enabled.

Default	disabled

Format	<code>dos-control icmpfrag</code>

Mode	Global Config

`no dos-control icmpfrag`

This command disables ICMP Fragment Denial of Service protection.

Format	<code>no dos-control icmpfrag</code>

Mode	Global Config

`dos-control vlan0tagged-snap`

M4250

M4350

This command enables the vlan0-tagged and snap mode to forward or drop vlan0-tagged packets and snap packets for security measures..

Default	disabled

Format	<code>dos-control vlan0tagged-snap</code>

Mode	Global Config

no dos-control vlan0tagged-snap

This command disables the vlan0-tagged and snap mode.

Format	no dos-control vlan0tagged-snap

Mode	Global Config

show dos-control

M4250

M4350

This command displays Denial of Service configuration information.

Format	show dos-control

Mode	Global Config Privileged EXEC

Term	Definition
Port D-disable mode	The port is administratively down. By default, this option is disabled.
First Fragment Mode	The administrative mode of First Fragment DoS prevention. If enabled, the switch drops packets that have a TCP header smaller than the configured Min TCP Hdr Size.
Min TCP Hdr Size	The minimum TCP header size that is accepted if First Fragment DoS prevention is enabled.
ICMPv4 Mode	The administrative mode of ICMPv4 DoS prevention. If enabled, the switch drops ICMP packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv4 Payload Size.
Max ICMPv4 Payload Size	The maximum ICMPv4 payload size that is accepted if ICMPv4 DoS protection is enabled.
ICMPv6 Mode	The administrative mode of ICMPv6 DoS prevention. If enabled, the switch drops ICMP packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv6 Payload Size.
Max ICMPv6 Payload Size	The maximum ICMPv6 payload size that is accepted if ICMPv6 DoS protection is enabled.
ICMPv4 Fragment Mode	The administrative mode of ICMPv4 Fragment DoS prevention. If enabled, the switch drops fragmented ICMPv4 packets.
TCP Port Mode	The administrative mode of TCP Port DoS prevention. If enabled, the switch drops packets that have the TCP source port equal to the TCP destination port.
UDP Port Mode	The administrative mode of UDP Port DoS prevention. If enabled, the switch drops packets that have the UDP source port equal to the UDP destination port.
SIPDIP Mode	The administrative mode of SIP=DIP DoS prevention. If enabled, the switch drops packets that have a source IP address equal to the destination IP address.

Term	Definition
SMACDMAC Mode	The administrative mode of SMAC=DMAC DoS prevention. If enabled, the switch drops packets that have a source MAC address equal to the destination MAC address.
TCP FIN&URG& PSH Mode	The administrative mode of TCP FIN & URG & PSH DoS prevention. If enabled, the switch drops packets that have the TCP flags FIN, URG, and PSH set and TCP Sequence Number = 0.
TCP Flag & Sequence Mode	The administrative mode of TCP Flag DoS prevention. If enabled, the switch drops packets that have the TCP control flags set to 0 and TCP sequence number set to 0.
TCP SYN Mode	The administrative mode of TCP SYN DoS prevention. If enabled, the switch drops packets that have the TCP Flags SYN set.
TCP SYN & FIN Mode	The administrative mode of TCP SYN & FIN DoS prevention. If enabled, the switch drops packets that have the TCP Flags SYN and FIN set.
TCP Fragment Mode	The administrative mode of TCP Fragment DoS prevention. If enabled, the switch drops packets that have a TCP payload in which the IP payload length minus the IP header size is less than the minimum allowed TCP header size.
TCP Offset Mode	The administrative mode of TCP Offset DoS prevention. If enabled, the switch drops packets that have a TCP header Offset equal to 1.
Stacked VLAN0 tag drop mode	Packets are discarded if they contain stacked VLAN tags and the inner VLAN tag does not match an allowed list. By default, this option is disabled.

auto-dos

M4250

M4350

This command enables Auto-DoS on the switch. By default, Auto-Dos is disabled.

When you enable Auto-DoS, all denial of service (DoS) checks are activated. If the switch detects a DoS attack, the offending packets are copied to the CPU and Auto-DoS shuts down the port and moves the port to the diagnostically disabled state. To use the port again, you must manually reenale the port.

Format	auto-dos
Mode	Global Config

no auto-dos

This command disables Auto-DoS on the switch.

Format	no auto-dos
Mode	Global Config

show auto-dos

M4250

M4350

The output of this command shows whether Auto-DoS is enabled on the switch.

Format	show auto-dos
Mode	Global Config Privileged EXEC

MAC Database Commands

This section describes the commands you use to configure and view information about the MAC databases.

bridge aging-time

M4250

M4350

This command configures the forwarding database address aging time-out in seconds. The *seconds* parameter must be within the range of 10 to 1,000,000 seconds.

Default	3000
Format	bridge aging-time <i>seconds</i>
Mode	Global Config

no bridge aging-time

This command sets the forwarding database address aging time-out to the default value.

Format	no bridge aging-time
Mode	Global Config

show forwardingdb agetime

M4250

M4350

This command displays the timeout for address aging.

Default	all
Format	show forwardingdb agetime
Mode	Privileged EXEC
Term	Definition
Address Aging Timeout	Displays the system's address aging timeout value in seconds.

show mac-address-table multicast

M4250

M4350

This command displays the Multicast Forwarding Database (MFDB) information. If you enter the command without a MAC address, the entire table is displayed. You can display the table entry for one MAC Address by specifying the MAC address as an optional parameter.

Format	show mac-address-table multicast [acaddr]
Mode	Privileged EXEC
Term	Definition
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Source	The component that is responsible for this entry in the Multicast Forwarding Database. The source can be IGMP Snooping, GMRP, and Static Filtering.
Type	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.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).
Fwd Interface	The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

Command example:

If one or more entries exist in the multicast forwarding table, the output is similar to the following:

```
(NETGEAR Switch) #show mac-address-table multicast
```

VLAN ID	MAC Address	Source	Type	Description	Interface	Fwd Interface
1	01:00:5E:01:02:03	Filter	Static	Mgmt Config	Fwd:	Fwd:
					1/0/1,	1/0/1,
					1/0/2,	1/0/2,
					1/0/3,	1/0/3,
					1/0/4,	1/0/4,
					1/0/5,	1/0/5,
					1/0/6,	1/0/6,
					1/0/7,	1/0/7,
					1/0/8,	1/0/8,
					1/0/9,	1/0/9,
					1/0/10,	1/0/10,

show mac-address-table stats

M4250

M4350

This command displays the Multicast Forwarding Database (MFDB) statistics.

Format show mac-address-table stats

Mode Privileged EXEC

Term	Definition
Total Entries	The total number of entries that can possibly be in the Multicast Forwarding Database table.
Most MFDB Entries Ever Used	The largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.
Current Entries	The current number of entries in the MFDB.

ISDP Commands

This section describes the commands you use to configure the industry standard Discovery Protocol (ISDP).

isdp run

M4250

M4350

This command enables ISDP on the switch.

Default	Enabled
Format	isdp run
Mode	Global Config

no isdp run

This command disables ISDP on the switch.

Format	no isdp run
Mode	Global Config

isdp holdtime

M4250

M4350

This command configures the hold time for ISDP packets that the switch transmits. The hold time specifies how long a receiving device should store information sent in the ISDP packet before discarding it. The period is in the range 10–255 seconds.

Default	180 seconds
Format	isdp holdtime <i>seconds</i>
Mode	Global Config

isdp timer

M4250

M4350

This command sets the period of time between sending new ISDP packets. The period is in the range 5–254 seconds.

Default	60 seconds
Format	<code>isdp timer seconds</code>
Mode	Global Config

isdp advertise-v2

M4250

M4350

This command enables the sending of ISDP version 2 packets from the device.

Default	Enabled
Format	<code>isdp advertise-v2</code>
Mode	Global Config

no isdp advertise-v2

This command disables the sending of ISDP version 2 packets from the device.

Format	<code>no isdp advertise-v2</code>
Mode	Global Config

isdp enable

M4250

M4350

This command enables ISDP on an interface or range of interfaces.

Note: ISDP must be enabled both globally and on the interface in order for the interface to transmit ISDP packets. If ISDP is globally disabled on the switch, the interface will not transmit ISDP packets, regardless of the ISDP status on the interface. To enable ISDP globally, use the command `isdp run` on page 845.

Default	Enabled
Format	<code>isdp enable</code>
Mode	Interface Config

no isdp enable

This command disables ISDP on the interface.

Format	<code>no isdp enable</code>
Mode	Interface Config

clear isdp counters

M4250

M4350

This command clears ISDP counters.

Format	<code>clear isdp counters</code>
Mode	Privileged EXEC

clear isdp table

M4250

M4350

This command clears entries in the ISDP table.

Format	<code>clear isdp table</code>
Mode	Privileged EXEC

show isdp

M4250

M4350

This command displays global ISDP settings.

Format	show isdp
Mode	Privileged EXEC
Term	Definition
Timer	The frequency with which this device sends ISDP packets. This value is in seconds.
Hold Time	The length of time the receiving device should save information sent by this device. This value is in seconds.
Version 2 Advertisements	The setting for sending ISDPv2 packets. If disabled, version 1 packets are transmitted.
Neighbors table time since last change	The amount of time that has passed since the ISPD neighbor table changed.
Device ID	The Device ID advertised by this device. The format of this Device ID is characterized by the value of the Device ID Format object.
Device ID Format Capability	Indicates the Device ID format capability of the device. - serialNumber indicates that the device uses a serial number as the format for its Device ID. - macAddress indicates that the device uses a Layer 2 MAC address as the format for its Device ID. - other indicates that the device uses its platform-specific format as the format for its Device ID.
Device ID Format	Indicates the Device ID format of the device. - serialNumber indicates that the value is in the form of an ASCII string containing the device serial number. - macAddress indicates that the value is in the form of a Layer 2 MAC address. - other indicates that the value is in the form of a platform specific ASCII string containing info that identifies the device. For example, ASCII string contains serialNumber appended/prepended with system name.

Command example:

```
(NETGEAR Switch) #show isdp
```

```

Timer..... 30
Hold Time..... 180
Version 2 Advertisements..... Enabled
Neighbors table time since last change..... 0 days 00:00:00
Device ID..... 1114728
Device ID format capability..... Serial Number, Host Name
Device ID format..... Serial Number

```

show isdp interface

M4250

M4350

This command displays ISDP settings for all interfaces or a specific interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	show isdp interface {all <i>unit/slot/port</i> }

Mode	Privileged EXEC

Term	Definition
Interface	The <i>unit/slot/port</i> of the specified interface.
Mode	ISDP mode enabled/disabled status for the interface(s).

Command example:

```
(NETGEAR Switch) #show isdp interface 0/1
```

Interface	Mode
-----	-----
0/1	Enabled

Command example:

```
(NETGEAR Switch) #show isdp interface all
```

Interface	Mode
-----	-----
0/1	Enabled
0/2	Enabled
0/3	Enabled
0/4	Enabled
0/5	Enabled
0/6	Enabled
0/7	Enabled
0/8	Enabled

show isdp entry

M4250

M4350

This command displays ISDP entries. If the *device-id* is specified, then only entries for that device are shown.

Format	show isdp entry {all <i>device-id</i> }
Mode	Privileged EXEC
Term	Definition
Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP address(es) associated with the neighbor.
Capability	ISDP Functional Capabilities advertised by the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (unit/slot/port) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Version	The software version that the neighbor is running.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Entry Last Changed Time	The time when the entry was last changed.

Command example:

```
(NETGEAR Switch) #show isdp entry Switch
```

```
Device ID                Switch

Address(es) :
IP Address:              172.20.1.18
IP Address:              172.20.1.18
Capability               Router IGMP
Platform                Netgear M4350
Interface                0/1
Port ID                 GigabitEthernet1/1
Holdtime                 64
Advertisement            Version 2
Entry last changed time  0 days 00:13:50
```

show isdp neighbors

M4250

M4350

This command displays the list of neighboring devices for all interfaces or for a specific interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format show isdp neighbors [*unit/slot/port* | detail]

Mode Privileged EXEC

Term	Definition
Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP addresses associated with the neighbor.
Capability	ISDP functional capabilities advertised by the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (<i>unit/slot/port</i>) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Entry Last Changed Time	Time when the entry was last modified.
Version	The software version that the neighbor is running.

Command example:

```
(NETGEAR Switch) #show isdp neighbors
```

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge,

S - Switch, H - Host, I - IGMP, r - Repeater

Device ID	Intf	Holdtime	Capability	Platform	Port ID
-----	----	-----	-----	-----	-----
Switch	0/1	165	RI	cisco WS-C4948	GigabitEthernet1/1

Command example:

```
(NETGEAR Switch) #show isdp neighbors detail
```

Fully Managed Switches M4250 and M4350 Series

```
Device ID          0001f45f1bc0
Address(es) :
IP Address:        10.27.7.57
Capability          Router Trans Bridge Switch IGMP
Platform           SecureChassis C2
Interface           0/48
Port ID             ge.3.14
Holdtime            131
Advertisement Version 2
Entry last changed time 0 days 00:01:59
Version:            05.00.56
```

show isdp traffic

M4250

M4350

This command displays ISDP statistics.

Format show isdp traffic

Mode Privileged EXEC

Term	Definition
ISDP Packets Received	Total number of ISDP packets received
ISDP Packets Transmitted	Total number of ISDP packets transmitted
ISDPv1 Packets Received	Total number of ISDPv1 packets received
ISDPv1 Packets Transmitted	Total number of ISDPv1 packets transmitted
ISDPv2 Packets Received	Total number of ISDPv2 packets received
ISDPv2 Packets Transmitted	Total number of ISDPv2 packets transmitted
ISDP Bad Header	Number of packets received with a bad header
ISDP Checksum Error	Number of packets received with a checksum error
ISDP Transmission Failure	Number of packets which failed to transmit
ISDP Invalid Format	Number of invalid packets received
ISDP Table Full	Number of times a neighbor entry was not added to the table due to a full database
ISDP IP Address Table Full	Displays the number of times a neighbor entry was added to the table without an IP address.

Command example:

```
(NETGEAR Switch) #show isdp traffic
```

```
ISDP Packets Received..... 4253
ISDP Packets Transmitted..... 127
ISDPv1 Packets Received..... 0
ISDPv1 Packets Transmitted..... 0
ISDPv2 Packets Received..... 4253
ISDPv2 Packets Transmitted..... 4351
ISDP Bad Header..... 0
ISDP Checksum Error..... 0
ISDP Transmission Failure..... 0
ISDP Invalid Format..... 0
ISDP Table Full..... 392
ISDP IP Address Table Full..... 737
```

debug isdp packet**M4250****M4350**

This command enables tracing of ISDP packets processed by the switch. ISDP must be enabled on both the device and the interface in order to monitor packets for a particular interface.

Note: To display the debug trace, enable the debug console command.

Format	debug isdp packet [receive transmit]

Mode	Privileged EXEC

no debug isdp packet

This command disables tracing of ISDP packets on the receive or the transmit sides or on both sides.

Format	no debug isdp packet [receive transmit]

Mode	Privileged EXEC

Interface Error Disabling and Auto Recovery Commands

Interface error disabling automatically disables an interface when an error is detected. No traffic is allowed until the interface is either manually reenabled or, if auto recovery is configured, the configured auto recovery interval expires.

If an error condition is detected for an interface, the switch places the interface in an error-disabled state (also referred to as a diagnostic-disabled state) by shutting down the interface. The error-disabled interface does not allow any traffic until the interface is reenabled. You can manually enable the error-disabled interface. Alternatively, you can enable auto recovery, which automatically reenables the interface after the expiration of the configured interval.

errdisable recovery cause

M4250

M4350

This command enables auto recovery for a specific cause or for all causes. If auto recovery is enabled, interfaces in the error-disabled state are reenabled when the recovery interval expires. If errors continue on the interface, the interface can be placed back in the error-disabled state and disabled. You can manually reenable an interface in the error-disabled state by entering the **no shutdown** command for the interface.

Format	errdisable recovery cause {all arp-inspection authmgr bcast-storm bpduguard bpdustorm coa denial-of-service dhcp-rate-limit keepalive link-flap mac-locking mcast-storm ucast-storm udld}
Mode	Global Config

no errdisable recovery cause

Use this command to disable auto recovery for a specific cause or for all causes. When disabled, interfaces that are in an error-disabled state do not recover automatically.

Format	errdisable recovery cause {all arp-inspection authmgr bcast-storm bpduguard bpdustorm coa denial-of-service dhcp-rate-limit keepalive link-flap mac-locking mcast-storm ucast-storm udld}
Mode	Global Config

errdisable recovery interval

M4250

M4350

Use this command to configure the auto recovery period, which is used for all causes. The period can be from 30 to 86400 seconds. When the recovery period expires, the switch attempts to bring interfaces in the error-disabled state back into service.

Default	300 seconds
Format	<code>errdisable recovery interval <i>period</i></code>
Mode	Global Config

no errdisable recovery interval

Use this command to reset the auto recovery period to the default period of 300 seconds.

Format	<code>no errdisable recovery interval</code>
Mode	Global Config

show errdisable recovery

M4250

M4350

Use this command to display whether auto recovery is enabled for the various features for which it can be enabled.

Format	<code>show errdisable recovery</code>
Mode	Privileged EXEC

Term	Definition
dhcp-rate-limit	Auto recovery is enabled or disabled for rate limiting of the DHCP Snooping feature.
arp-inspection	Auto recovery is enabled or disabled for the ARP Inspection feature.
udld	Auto recovery is enabled or disabled for the UDLD feature.
bcast-storm	Auto recovery is enabled or disabled for the broadcast storm conditions.
mcast-storm	Auto recovery is enabled or disabled for the multicast storm conditions.
ucast-storm	Auto recovery is enabled or disabled for the unicast storm conditions.
bpdguard	Auto recovery is enabled or disabled for the BPDU Guard feature.
bpdustorm	Auto recovery is enabled or disabled for BPDU storm conditions.
keep-alive	Auto recovery is enabled or disabled for keep-alive conditions.

Term	Definition
mac-locking	Auto recovery is enabled or disabled for port MAC locking conditions.
denial-of-service	Auto recovery is enabled or disabled for DoS conditions.
link-flap	Auto recovery is enabled or disabled for the link-flap conditions.
authmgr	Auto recovery is enabled or disabled for 802.1x and MAB authentications.
coa	Auto recovery is enabled or disabled for Change of Authorization (CoA) conditions.

Command example:

```
(NETGEAR Switch) #show errdisable recovery
```

```
Errdisable Reason      Auto-recovery Status
-----
dhcp-rate-limit        Disabled
arp-inspection          Disabled
udld                    Disabled
bcast-storm             Disabled
mcast-storm             Disabled
ucast-storm             Disabled
bpduguard              Disabled
bpdustorm              Disabled
keepalive               Disabled
mac-locking             Disabled
denial-of-service       Disabled
link-flap               Disabled
authmgr                 Disabled
coa                     Disabled
Timeout for Auto-recovery from D-Disable state 300
```

show interfaces status err-disabled**M4250****M4350**

Use this command to display the interfaces that are error-disabled, the reason they are error-disabled, and the period remaining before auto recovery occurs.

Format	show interfaces status err-disabled
Mode	Privileged EXEC

Term	Definition
interface	An interface that is error-disabled.
Errdisable Reason	The reason the interface is error-disabled.
Auto-Recovery Time Left	The period that is remaining before auto recovery occurs.

Command example:

```
(NETGEAR Switch) #show interfaces status err-disabled
```

Interface	Errdisable Reason	Auto-Recovery Time Left(sec)
0/1	udld	279
0/2	bpduguard	285
0/3	bpdustorm	291
0/4	keepalive	11

UniDirectional Link Detection Commands

The purpose of the UniDirectional Link Detection (UDLD) feature is to detect and avoid unidirectional links. A unidirectional link is a forwarding anomaly in a Layer 2 communication channel in which a bi-directional link stops passing traffic in one direction. Use the UDLD commands to detect unidirectional links' physical ports. UDLD must be enabled on both sides of the link in order to detect a unidirectional link. The UDLD protocol operates by exchanging packets containing information about neighboring devices.

udld enable (Global Config)

M4250

M4350

This command enables UDLD globally on the switch.

Default	Disabled
Format	udld enable
Mode	Global Config

no udld enable (Global Config)

This command disables UDLD globally on the switch.

Format	no udld enable
Mode	Global Config

udld message time

M4250**M4350**

This command configures the interval between UDLD probe messages on ports that are in the advertisement phase. The range is from 1 to 90 seconds.

Default	15 seconds
Format	<code>udld message time <i>seconds</i></code>
Mode	Global Config

udld timeout interval

M4250**M4350**

This command configures the time interval after which UDLD link is considered to be unidirectional. The range is from 3 to 60 seconds.

Default	5 seconds
Format	<code>udld timeout interval <i>seconds</i></code>
Mode	Global Config

udld enable (Interface Config)

M4250**M4350**

This command enables UDLD on the specified interface.

Default	disable
Format	<code>udld enable</code>
Mode	Interface Config

no udld enable (Interface Config)

This command disables UDLD on the specified interface.

Format	<code>no udld enable</code>
Mode	Interface Config

udld reset

M4250**M4350**

This command resets all interfaces that have been shutdown by UDLD.

Default	None
Format	udld reset
Mode	Privileged EXEC

udld port

M4250**M4350**

This command selects the UDLD mode operating on this interface. If the **aggressive** keyword is not entered, the port operates in normal mode.

Default	normal
Format	udld port [aggressive]
Mode	Interface Config

show udld

M4250**M4350**

This command displays either the global settings of UDLD or the UDLD settings for the specified interface. If you enter the **all** keyword, the command output displays information for all ports. If you enter the **internal** keyword, the command output displays UDLD statistics. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	show udld [<i>unit/slot/port</i> <i>all</i> <i>internal</i>]
Mode	User EXEC Privileged EXEC

If you do not enter a value for the *unit/slot/port* parameter, the command output displays the fields that are shown in the following table.

Parameter	Description
Admin Mode	The global administrative mode of UDLD.
Message Interval	The time period (in seconds) between the transmission of UDLD probe packets.
Timeout Interval	The time period (in seconds) before making a decision that the link is unidirectional.

If you enter a value for the *unit/slot/port* parameter or you use the **all** keyword, the command output displays the fields that are shown in the following table.

Parameter	Description
Port	The identifying port of the interface.
Admin Mode	The administrative mode of UDLD configured on this interface. This is either Enabled or Disabled.
UDLD Mode	The UDLD mode configured on this interface. This is either Normal or Aggressive.
UDLD Status	The status of the link as determined by UDLD. The options are: • Undetermined. UDLD has not collected enough information to determine the state of the port. • Not applicable. UDLD is disabled, either globally or on the port. • Shutdown. UDLD has detected a unidirectional link and shutdown the port. That is, the port is in an errDisabled state. • Bidirectional. UDLD has detected a bidirectional link. • Undetermined (Link Down). The port would transition into this state when the port link physically goes down due to any reasons other than the port been put into D-Disable mode by the UDLD protocol on the switch.

Command example:

The following output displays after you enable UDLD and configure nondefault interval values:

```
(NETGEAR Switch) #show udld
```

```
Admin Mode..... Enabled
Message Interval..... 13
Timeout Interval..... 31
```

Command example:

```
(NETGEAR Switch) #show udld 0/1
```

```
Port      Admin Mode  UDLD Mode  UDLD Status
----      -
0/1       Enabled    Normal     Not Applicable
```


Command example:

```
(NETGEAR Switch) #show uddl all
```

Port	Admin Mode	UDLD Mode	UDLD Status
-----	-----	-----	-----
0/1	Enabled	Normal	Shutdown
0/2	Enabled	Normal	Undetermined
0/3	Enabled	Normal	Bidirectional
0/4	Enabled	Normal	Not Applicable
0/5	Enabled	Normal	Not Applicable
0/6	Enabled	Normal	Not Applicable
0/7	Enabled	Normal	Not Applicable
0/8	Enabled	Normal	Shutdown
0/9	Enabled	Normal	Not Applicable
0/10	Enabled	Normal	Not Applicable
0/11	Enabled	Normal	Not Applicable
0/12	Enabled	Normal	Undetermined
0/13	Enabled	Normal	Bidirectional
0/14	Disabled	Normal	Not Applicable
0/15	Disabled	Normal	Not Applicable
0/16	Disabled	Normal	Not Applicable
0/17	Disabled	Normal	Not Applicable
0/18	Disabled	Normal	Not Applicable
0/19	Disabled	Normal	Not Applicable
0/20	Disabled	Normal	Not Applicable

IPv4 Device Tracking Commands

The IPv4 Device Tracking (IPv4DT) feature enables you to track IPv4 hosts that are attached to physical ports or LAGs on an L2 or L3 switch.

The DHCP Snooping feature (see [DHCP Snooping Configuration Commands on page 718](#)) already provides mapping from host IP address to physical port on an L2 switch, for the IP address acquired using DHCP. But DHCP snooping cannot track the statically configured hosts, nor can it detect the movement of the hosts in a VLAN.

The IPv4 Device Tracking feature snoops the ARP packets exchanged in a VLAN and populates the tracking table with the information such as IP address, MAC address, VLAN ID, and interface number for each host.

ip device tracking (Global Config)

M4250**M4350**

This command enables the IPv4 Device Tracking feature.

Default	Disabled
Format	ip device tracking
Mode	Global Config

no ip device tracking (Global Config)

This command disables enables the IPv4 Device Tracking feature.

Format	no ip device tracking
Mode	Global Config

ip device tracking maximum (Interface Config)

M4250**M4350**

This command sets the maximum number of entries learned on a routing or non-routing interface. This command clears all entries that were learned on the interface and sets the maximum of entries (from 1 to 10) that can be learned on the interface. If you set the maximum entries to zero, IPv4DT is effectively disabled on the interface.

Default	No limit
Format	ip device tracking maximum <i>number</i>
Mode	Interface Config

no ip device tracking maximum (Interface Config)

This command resets the number of entries that can be learned on a or non-routing interface to the default, which is no limit.

Format	no ip device tracking maximum
Mode	Interface Config

clear ip device tracking

M4250**M4350**

Use this command to clear the entries present in the IPv4DT database. Specify arguments to clear based on interface name, IPv4 address, and MAC address. When you enter the command, the ARP probes are sent to repopulate the entries.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	<code>clear ip device tracking {all interface <i>unit/slot/port</i> ip <i>ip-address</i> mac <i>mac-address</i>}</code>

Mode	Privileged Config

Parameter	Description
all	Clears the entire IPv4DT table.
interface <i>unit/slot/port</i>	Clears the entries that were learned on a specified interface.
ip <i>ip-address</i>	Clears the entries that match the host IPv4 address.
mac <i>mac-address</i>	Clears the entries that match the MAC address.

ip device tracking probe

M4250**M4350**

This command enables the ARP probe generation for each entry in the IPv4 Device Tracking database.

Default	Enabled

Format	<code>ip device tracking probe</code>

Mode	Global Config

no ip device tracking probe

This command disables the ARP probe generation for each entry in the IPv4 Device Tracking database.

Format	no ip device tracking probe
Mode	Global Config

ip device tracking probe interval

M4250

M4350

This command sets the minimum time in seconds between two ARP probes for each entry in the IPv4 Device Tracking database. The range is from 30 to 300 seconds.

Default	30 seconds
Format	ip device tracking probe interval <i>seconds</i>
Mode	Global Config

no ip device tracking probe interval

This command resets the probe interval to the default of 30 seconds.

Format	no ip device tracking probe interval
Mode	Global Config

ip device tracking probe count

M4250

M4350

This command sets the number of probes sent without any responses from the client before declaring that its state is inactive in the IPv4 Device Tracking database. The range for the *number* argument is from 1 to 255.

Default	3
Format	ip device tracking probe count <i>number</i>
Mode	Global Config

no ip device tracking probe interval

This command resets the probe count to the default of 3.

Format	no ip device tracking probe count

Mode	Global Config

ip device tracking probe delay

M4250

M4350

This command sets the delay in seconds before the probe is sent after a port is moving from the non-forwarding state to the forwarding state. This delay applies to each entry in the IPv4 Device Tracking database. The range is from 1 to 120 seconds.

Default	30 seconds

Format	ip device tracking probe delay <i>number</i>

Mode	Global Config

no ip device tracking probe delay

This command resets the probe delay to the default of 30 seconds.

Format	no ip device tracking probe delay

Mode	Global Config

ip device tracking probe auto-source fallback

M4250

M4350

This command sets the source address in the ARP probe packet for non-routing interfaces to prevent the duplication of IP address 0.0.0.0. When you enter the command, the source address in the probe packet is set to a new address based on the configured host IP address, mask, and the destination for each of the non-routing interfaces in the IPv4DT table.

Default	The source IP address in the probe packet for non-routing interfaces is 0.0.0.0.

Format	ip device tracking probe auto-source fallback <i>host-ip mask</i> override

Mode	Global Config

Parameter	Description
<i>host-ip</i>	An IPv4 host in dotted notation (for example, 1.2.3.4).
<i>mask</i>	An IPv4 host used for the destination IP address of the IPv4DT entries in dotted notation (for example, 255.255.0.0).

Command example:

In the following example, the probe entry for a host IP address is 10.5.5.20, causing an ARP probe with source address 10.5.5.1 to be generated:

```
(NETGEAR Switch) (Config) # ip device tracking probe auto-source fallback 0.0.0.1
255.255.255.0 override
```

```
no ip device tracking probe auto-source fallback
```

This command resets the source address in the ARP probe packet for non-routing interfaces to the default of 0.0.0.0.

Format	no ip device tracking probe auto-source fallback
Mode	Global Config

```
show ip device tracking all
```

M4250

M4350

This command displays all IPv4DT (IPv4, VLAN, and MAC) entries in the IPv4DT table.

Format	show ip device tracking all [count active inactive]
Mode	Privileged Config

Parameter	Description
active	(Optional) Displays the active status entries only.
inactive	(Optional) Displays the inactive status entries only.
count	(Optional) Displays the number of ARP, DHCP, active, and inactive IPv4DT entries in the IPv4DT table.

Command example:

```
(NETGEAR Switch) #show ip device tracking all
```

```
IP Device Tracking for clients..... Enable
IP Device Tracking Probe Generation..... Enable
IP Device Tracking Probe Count..... 3
IP Device Tracking Probe Interval.....30
```

Fully Managed Switches M4250 and M4350 Series

```
IP Device Tracking Probe Delay Interval.....30
```

```
-----  
IP Address  MAC Address      Vlan Interface Time-left   Time-since State Source  
                        to inactive inactive  
-----
```

```
10.21.1.1   01:02:03:04:05:06  2   1/0/1      30         0      ACTIVE  ARP
```

```
Total number interfaces enabled: 1
```

```
Enabled interfaces:
```

```
1/0/1
```

Command example:

```
(NETGEAR Switch) #show ip device tracking all count
```

```
IP Device Tracking ARP Entries Count ..... 40
```

```
IP Device Tracking DHCP Entries Count ..... 0
```

```
IP Device Tracking ACTIVE Entries Count ..... 30
```

```
IP Device Tracking INACTIVE Entries Count ..... 10
```

```
IP Device Tracking Total Entries Count ..... 40
```

show ip device tracking interface

M4250

M4350

This command displays all IPv4DT (IPv4, VLAN, and MAC) entries in the IPv4DT table learned on a specific interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	<code>show ip device tracking interface <i>unit/slot/port</i></code>

Mode	Privileged Config

Field	Description
IP Address	The learned IPv4 address of the device.
MAC Address	The MAC address associated with the learned IPv4 address.
VLAN	The VLAN ID associated with an interface on which the device is learned.
Interface	The interface number on which the device is learned.

Field	Description
State	Indicates if the device is in the active or inactive state.
Time left to inactive	The number of seconds before the reachable device is set to inactive.
Time since inactive	The number of seconds since the inactive device was last reachable.
Source	Indicates if the source of the device is ARP, DHCP, or static.

Command example:

```
(Switching) #show ip device tracking interface 1/0/1
```

```
IP Device Tracking for clients..... Enable
IP Device Tracking Probe Generation..... Enable
IP Device Tracking Probe Count..... 3
IP Device Tracking Probe Interval.....30
IP Device Tracking Probe Delay Interval.....30
IP Device Tracking Interface Max Entry Limit .....No Limit
```

```
-----
IP Address  MAC Address      Vlan Interface Time-left   Time-since State Source
                        to inactive inactive
-----
10.21.1.1   01:02:03:04:05:06  2   1/0/1      50         0      ACTIVE  ARP
20.21.1.1   01:02:03:04:05:07  2   1/0/1      80         0      ACTIVE  ARP
```

show ip device tracking ip**M4250****M4350**

This command displays all IPv4DT (IPv4, VLAN, and MAC) entries in the IPv4DT table learned on a specific IPv4 address.

Format	<code>show ip device tracking ip <i>ip-address</i></code>

Mode	Privileged Config

Field	Description
IP Address	The learned IPv4 address of the device.
MAC Address	The MAC address associated with the learned IPv4 address.
VLAN	The VLAN ID associated with an interface on which the device is learned.
Interface	The interface number on which the device is learned.
Time left to inactive	The number of seconds before the reachable device is set to inactive.

Fully Managed Switches M4250 and M4350 Series

Field	Description
Time since inactive	The number of seconds since the inactive device was last reachable.
State	Indicates if the device is in the active or inactive state.
Source	Indicates if the source of the device is ARP, DHCP, or static.

Command example:

```
(Switching) #show ip device tracking ip 10.21.1.1
```

```
IP Device Tracking for clients..... Enable
IP Device Tracking Probe Generation..... Enable
IP Device Tracking Probe Count..... 3
IP Device Tracking Probe Interval.....30
IP Device Tracking Probe Delay Interval.....30
-----
IP Address  MAC Address      Vlan Interface Time-left  Time-since State Source
                        to inactive inactive
-----
10.21.1.1   01:02:03:04:05:06  2   1/0/1      50         0    ACTIVE  ARP
10.21.1.1   01:02:03:04:05:07  2   1/0/2      50         0    ACTIVE  ARP
```

show ip device tracking mac

M4250

M4350

This command displays all IPv4DT (IPv4, VLAN, and MAC) entries in the IPv4DT table learned for a specific MAC address.

Format	<code>show ip device tracking mac <i>mac-address</i></code>
Mode	Privileged Config

Field	Description
IP Address	The learned IPv4 address of the device.
MAC Address	The MAC address associated with the learned IPv4 address.
VLAN	The VLAN ID associated with an interface on which the device is learned.
Interface	The interface number on which the device is learned.
Time left to inactive	The number of seconds before the reachable device is set to inactive.
Time since inactive	The number of seconds since the inactive device was last reachable.

Field	Description
State	Indicates if the device is in the active or inactive state.
Source	Indicates if the source of the device is ARP, DHCP, or static.

Command example:

```
(Switching) #show ip device tracking mac 01:02:03:04:05:06
```

```
IP Device Tracking for clients..... Enable
IP Device Tracking Probe Generation..... Enable
IP Device Tracking Probe Count..... 3
IP Device Tracking Probe Interval.....30
IP Device Tracking Probe Delay Interval.....30
-----
IP Address  MAC Address      Vlan Interface Time-left   Time-since State Source
                        to inactive inactive
-----
10.21.1.1   01:02:03:04:05:06  2   1/0/1        50           0      ACTIVE  ARP
20.21.1.1   01:02:03:04:05:06  2   1/0/1        50           0      ACTIVE  ARP
```

Link Debounce Commands

Link debouncing functions on a per-port basis on physical interfaces. After you configure link debouncing, if the switch receives a link-down notification, the switch starts monitoring the link event by starting a timer with the configured debounce time. Any intermediate link-down and link-up events are ignored hereafter. When the timer expires, link debounce checks if the current state of the link is still down; if so, it forwards a link-down notification to the upper layer applications.

You must explicitly enable link debounce per interface with an appropriate debounce timer value, taking into consideration the network topology and the features enabled on the switch, such as LAG or spanning tree.

Note: Link debouncing is disabled by default.

link debounce time

M4250

M4350

This command configures the debounce time. The possible values for the *milliseconds* parameter are in the 100–5000 range.

Format	link debounce time <i>milliseconds</i>

Mode	Interface Config

no link debounce time

This command disables the debounce time.

Format	no link debounce time

Mode	Interface Config

show interface debounce

M4250

M4350

This command displays the flap counts for all interfaces.

Format	show interface debounce

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show interface debounce
```

Interface	Debounce Time(ms)	Flaps
-----	-----	-----
1/0/1	0	0
1/0/2	0	0
1/0/3	0	0
1/0/4	0	0
1/0/5	0	0
1/0/6	0	0

Bonjour Commands

A Mac that supports Bonjour can discover the switch in the network so that you can find the switch IP address and log in to the local browser user interface of the switch. Bonjour is enabled by default on the switch. You can disable Bonjour for security reasons.

bonjour run

M4250

M4350

This command enables Bonjour on the switch.

Default	Enabled
Format	<code>bonjour run</code>
Mode	Global Config

no bonjour run

This command disables Bonjour on the switch.

Format	<code>no bonjour run</code>
Mode	Global Config

show bonjour

M4250

M4350

This command displays the Bonjour information and the published services.

Format	<code>show bonjour</code>
Mode	Privileged EXEC

Term	Definition
Service Name	The Bonjour service name on the switch.
Type	The Bonjour service type name on the switch.
Domain	The Bonjour service domain name on the switch.
Port	The Bonjour service port number on the switch.
TXT data	The Bonjour service text on the switch.

Command example:

```
(Netgear Switch) #show bonjour
Bonjour Administration Mode: Enabled
Published Services:
```

#	Service Name	Type	Domain	Port	TXT data
1	M4350-12X12F	192.168.100.118	_http._tcp.	local.	80 path=/ 23
2	M4350-12X12F	192.168.100.118	_telnet._tcp.	local.	

debug bonjour**M4250****M4350**

This command enables Bonjour tracing. As an option, you can set level 1 or level 2 debugging.

Default	Disabled
Format	debug bonjour [level1 level2]
Mode	Privileged Config

no debug bonjour

This command disables all previously enabled Bonjour debug traces.

Format	debug bonjour [level1 level2]
Mode	Privileged Config

Audio Video Bridging Commands

Note: Audio-video bridging (AVB) and Precision Time Protocol (PTP)-transparent clocks (TC) are mutually exclusive. You can either specify the settings for 802.1AS and MRP, both of which configure the switch for AVB and are described in this section, or specify the settings for PTP-TC (see [Precision Time Protocol Commands on page 572](#)).

The AVB protocol suite includes the following protocols:

- **IEEE 802.1AS-2011.** IEEE 802.1AS-2011 Timing and Synchronization for Time-Sensitive Applications (generalized Precision Time Protocol [gPTP])
- **IEEE 802.1Qav-2009.** Forwarding and Queuing for Time-Sensitive Streams (FQTSS)

- **IEEE 802.1Qat-2010.** Stream Reservation Protocol (SRP)
- **IEEE 802.1BA-2011.** Audio Video Bridging (AVB) Systems
- **IEEE 1722-2011.** Layer 2 Transport Protocol for Time Sensitive Applications (AV Transport Protocol [AVTP])

The M4350 series switch supports the following Multiple Registration Protocol (MRP) protocols:

- **MMRP.** Multiple MAC Registration Protocol (MMRP) registers MAC address information.
- **MVRP.** Multiple VLAN Registration Protocol (MVRP) registers VLAN membership.
- **MSRP.** Multiple Stream Reservation Protocol (MSRP) registers bandwidth requirement for an AV stream.

MRP lets devices register attributes to other devices in a network. MRP is the base registration protocol that is then used by MMRP and MSRP to propagate the registration.

MRP replaces Generic Attribute Registration Protocol (GARP), which is still supported on the switch. The following related protocols are also replaced:

- GARP Multicast Registration Protocol (GMRP) is replaced by MMRP but still supported on the switch.
- GARP VLAN Registration Protocol (GVRP) is replaced by MVRP but still supported on the switch.

802.1AS Commands

802.1AS can ensure that QoS requirements are guaranteed for time-sensitive applications such as audio and video. Precision Time Protocol (PTP) forms the basis for 802.1AS. PTP can provide precise clock synchronization that relies on time-stamped packets. PTP is applicable to a distributed system that consist of one or more communicating nodes. The distribution of synchronous time information occurs hierarchically with a grandmaster clock. The grandmaster clock provides a common and precise time reference by exchanging timing information with one or more directly-attached devices. Such an attached device synchronizes its clocks with the grandmaster clock and, in turn, can function as master clock for a hierarchical layer of attached devices.

Time synchronization provides a common time base for sampling data streams at a source device and presenting those streams at a destination device with the same relative timing. End-to-end synchronization of clocks is critical for traffic that is highly time-sensitive with stringent latency and jitter requirements.

802.1AS supports the following:

- Network clock synchronization in the sub-microsecond range
- Synchronization of clocks with different precision, resolution and stability
- Fast convergence when topology changes occur

dot1as

M4250

M4350

This command enables 802.1AS on the switch.

Default	Disabled
Format	dot1as
Mode	Global Config

no dot1as

This command disables 802.1AS on the switch.

Format	no dot1as
Mode	Global Config

dot1as priority 1

M4250

M4350

This command configures the 802.1AS priority 1 value for the switch.

Default	248
Format	dot1as priority 1 value
Mode	Global Config

Parameter	Description
value	The value for the best clock priority is in the range from 0 to 255. The default value is 248.

no dot1as priority 1

This command sets the 802.1AS priority 1 value for the switch to its default setting of 248.

Format	no dot1as 1 priority
Mode	Global Config

dot1as priority 2

This command configures the 802.1AS priority 2 value for the switch.

Default	248
Format	<code>dot1as priority 2 value</code>
Mode	Global Config

Parameter	Description
value	The value for the best clock priority is in the range from 0 to 255. The default value is 248.

no dot1as priority 2

This command sets the 802.1AS priority 2 value for the switch to its default setting of 248.

Format	<code>no dot1as 2 priority</code>
Mode	Global Config

dot1as interval announce

M4250

M4350

This command configures the initial mean time interval between successive Announce messages in the format of logarithms to base 2 (log base 2). The value of *interval* can be from –5 to 5.

Default	0
Format	<code>dot1as interval announce interval</code>
Mode	Interface Config

no dot1as interval announce

This command sets the initial mean time interval between successive Announce messages to its default value of 0.

Format	<code>no dot1as interval announce</code>
Mode	Interface Config

dot1as interval sync

M4250**M4350**

This command configures the initial mean time interval between successive Sync messages in the format of logarithms to base 2 (log base 2). The value of *interval* can be from –5 to 5.

Default	0
Format	dot1as interval sync <i>interval</i>
Mode	Interface Config

no dot1as interval sync

This command sets the initial mean time interval between successive Sync messages to its default value of 0.

Format	no dot1as interval sync
Mode	Interface Config

dot1as interval pdelay

M4250**M4350**

This command configures the initial mean time interval between successive Pdelay messages in the format of logarithms to base 2 (log base 2). The value of *interval* can be from –5 to 5.

Default	0
Format	dot1as interval pdelay <i>interval</i>
Mode	Config

no dot1as interval pdelay

This command sets the initial mean time interval between successive Pdelay messages to its default value of 0.

Format	no dot1as interval pdelay
Mode	Interface Config

dot1as timeout announce

M4250

M4350

This command configures the number of Announce intervals that the switch accepts without receipt of an Announce message before it determines that the master clock stopped transmitting. The value of *number* can be from 2 to 255.

Default	3
Format	dot1as timeout announce <i>number</i>
Mode	Interface Config

no dot1as timeout announce

This command sets the number of Announce intervals that the switch accepts without receipt of an Announce message to its default value of 3.

Format	no dot1as timeout announce
Mode	Interface Config

dot1as timeout sync

M4250

M4350

This command configures the number of Sync intervals that the switch accepts without receipt of a Sync message before it determines that the master clock stopped transmitting. The value of *number* can be from 2 to 255.

Default	3
Format	dot1as timeout sync <i>number</i>
Mode	Interface Config

no dot1as timeout sync

This command sets the number of Sync intervals that the switch accepts without receipt of a Sync message to its default value of 3.

Format	no dot1as timeout sync
Mode	Interface Config

dot1as pdelay-threshold

M4250

M4350

This command configures the propagation delay threshold in nanoseconds, above which an interface is not considered capable of participating in the 802.1AS protocol. The value of nanoseconds can be from 0 to 1,000,000,000.

Default M4250	8000
Default M4350	3000
Format	dot1as pdelay-threshold <i>nanoseconds</i>
Mode	Interface Config

no dot1as pdelay-threshold

This command sets the propagation delay threshold in nanoseconds to its default value.

Format	no dot1as pdelay-threshold
Mode	Interface Config

dot1as allowedlostresp

M4250

M4350

This command configures the maximum number of Pdelay_Req messages for which the switch does not receive a response. Above that number, an interface is considered to not be exchanging peer delay messages with its neighbor. The value of *number* can be from 0 to 65535.

Default	3
Format	dot1as allowedlostresp <i>number</i>
Mode	Interface Config

no dot1as allowedlostresp

This command sets the maximum number of Pdelay_Req messages for which the switch does not receive a response to its default value of 3.

Format	no dot1as allowedlostresp
Mode	Interface Config

show dot1as summary

M4250

M4350

This command displays a summary of the 802.1AS configuration on the switch.

Format show dot1as summary

Mode Privileged EXEC

Term	Definition
802.1AS Global Admin Mode	Indicates if the 802.1AS global admin mode is enabled or disabled.
Grandmaster Capable	Indicates if the 802.1AS global admin mode is enabled or disabled.
Best Clock Identity	The clock identity of the 802.1AS grandmaster.
Best Clock Priority1	The priority1 value of the 802.1AS grandmaster.
Best Clock Priority2	The priority2 value of the 802.1AS grandmaster.
Steps to Best Clock	The number of hops between the local clock and the 802.1AS grandmaster.
Local Clock Identity	The clock identity of the 802.1AS local clock.
Local Clock Priority1	The priority1 value of the 802.1AS local clock.
Local Clock Priority2	The priority2 value of the 802.1AS local clock.
Grandmaster Change Count	The number of 802.1AS grandmaster change events that occurred.
Last Grandmaster Change Timestamp	The timestamp of the last grandmaster change event.

Command example:

```
(NETGEAR switch) (Config)#show dot1as summary
```

```
802.1AS Global Admin Mode..... Disabled
Grandmaster Capable..... No
Best Clock Identity..... 44:A5:6E:FF:FE:59:38:D0
Best Clock Priority1..... 255
Best Clock Priority2..... 248
Steps to Best Clock..... 0
Local Clock Identity..... 44:A5:6E:FF:FE:59:38:D0
Local Clock Priority1..... 255
Local Clock Priority2..... 248
Grandmaster Change Count..... 0
Last Grandmaster Change Timestamp..... 0
```

show dot1as interface

M4250

M4350

This command displays the 802.1AS configuration for all interfaces or for a specific interface or LAG. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	<code>show dot1as interface {summary unit/slot/port lag lag-intf-num}</code>

Mode	Privileged EXEC

The following information displays when you use the **summary** keyword.

Term	Definition
Intf	The interface.
Mode	Indicates if the 802.1AS interface admin mode is enabled or disabled.
asCapable	Indicates if the interface is 802.1AS-capable.
measuringPdelay	Indicates if the interface is measuring the propagation delay (Pdelay).
Pdelay	The propagation delay value on the interface.
Role	The 802.1AS role of the interface: timeTransmitter, timeReceiver, Passive, or Disabled.

The following information displays when you use the *unit/slot/port* parameter.

Term	Definition
802.1AS Interface Admin Mode	Indicates if the 802.1AS interface admin mode is enabled or disabled.
802.1AS Capable	Indicates if the interface is 802.1AS-capable.
Is Measuring Delay	Indicates if the interface is measuring delay.
Propagation Delay	The propagation delay value on the interface.
Port Role	The 802.1AS role of the interface: timeTransmitter, timeReceiver, Passive, or Disabled.
PDELAY Threshold	The propagation delay threshold in nanoseconds, above which an interface is not considered capable of participating in the 802.1AS protocol.
PDELAY lost responses allowed	The number of Pdelay_Req messages for which a valid response is not received, above which a port is considered to not be exchanging peer delay messages with its neighbor.
Neighbor Rate Ratio	An estimate of the ratio of the frequency of the LocalClock entity of the time-aware system at the other end of the link of the interface, to the frequency of the LocalClock entity of this time-aware switch.

Term	Definition
Initial Sync Interval	The configured mean time interval between successive PDELAY_REQ messages sent over the link, in logarithm to base 2 format.
Current Sync Interval	The current mean time interval between successive SYNC messages sent over the link, in logarithm to base 2 format.
Initial Pdelay Interval	The configured mean time interval between successive PDELAY_REQ messages sent over the link, in logarithm to base 2 format.
Current Pdelay Interval	The current mean time interval between successive PDELAY_REQ messages sent over the link, in logarithm to base 2 format.
Initial Announce Interval	The configured mean time interval between successive ANNOUNCE messages sent over the link, in logarithm to base 2 format.
Current Announce Interval	The current mean time interval between successive ANNOUNCE messages sent over the link, in logarithm to base 2 format.
Sync Receipt Timeout	The number of SYNC intervals that must pass without receipt of SYNC information before the master is considered to no longer transmit.
Announce Receipt Timeout	The number of ANNOUNCE intervals that must pass without receipt of ANNOUNCE PDU before the master is considered to no longer transmit.

Command example:

```
(NETGEAR Switch) (Config) #show dot1as interface summary
```

Intf	Mode	asCapable	measuringPdelay	Pdelay	Role
-----	-----	-----	-----	-----	-----
0/1	Disabled	No	No	0	Disabled
0/2	Disabled	No	No	0	Disabled
0/3	Disabled	No	No	0	Disabled
0/4	Disabled	No	No	0	Disabled
0/5	Disabled	No	No	0	Disabled
0/6	Disabled	No	No	0	Disabled
0/7	Disabled	No	No	0	Disabled
0/8	Disabled	No	No	0	Disabled
0/9	Disabled	No	No	0	Disabled
0/10	Disabled	No	No	0	Disabled
0/11	Disabled	No	No	0	Disabled
0/12	Disabled	No	No	0	Disabled
lag 1	Disabled	No	No	0	Disabled
lag 2	Disabled	No	No	0	Disabled
lag 3	Disabled	No	No	0	Disabled
lag 4	Disabled	No	No	0	Disabled
lag 5	Disabled	No	No	0	Disabled
lag 6	Disabled	No	No	0	Disabled
lag 7	Disabled	No	No	0	Disabled
lag 8	Disabled	No	No	0	Disabled

Command example:

```
(NETGEAR Switch) (Config)#show dot1as interface 0/7
```

```
802.1AS Interface Admin Mode..... Disabled
802.1AS Capable..... No
Is Measuring Delay..... No
Propagation Delay..... 0
Port Role..... Disabled
PDELAY Threshold..... 2500
PDELAY lost responses allowed..... 3
Neighbor Rate Ratio..... 0
Initial Sync Interval..... -3
Current Sync Interval..... 0
Initial Pdelay Interval..... 0
Current Pdelay Interval..... 0
Initial Announce Interval..... 0
Current Announce Interval..... 0
Sync Receipt Timeout..... 3
Announce Receipt Timeout..... 3
```

show dot1as statistics**M4250****M4350**

This command displays the 802.1AS configuration statistics for a specific interface or LAG. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	<code>show dot1as statistics {unit/slot/port lag lag-intf-num}</code>

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) (Config)#show dot1as statistics 0/2
```

```
Port..... 0/2
Sync messages transmitted..... 0
Sync messages received..... 0
Followup messages transmitted..... 0
Followup messages received..... 0
Announce messages transmitted..... 0
```

```

Announce messages received..... 0
Pdelay_Req messages transmitted..... 0
Pdelay_Req messages received..... 0
Pdelay_Resp messages transmitted..... 0
Pdelay_Resp messages received..... 0
Pdelay_Resp_Followup messages transmitted..... 0
Pdelay_Resp_Followup messages received..... 0
Signaling messages transmitted..... 0
Signaling messages received..... 0
Sync receipt timeouts..... 0
Sync messages discarded..... 0
Announce receipt timeouts..... 0
Announces messages discarded..... 0
Pdelay receipt timeouts..... 0
Pdelay messages discards..... 0
PTP message discards..... 0
Pdelay allowed lost responses..... 0
Invalid 802.1AS messages received..... 0

```

clear dot1as statistics

M4250

M4350

This command clear the 802.1AS configuration statistics for a specific interface or for all interfaces. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	clear dot1as statistics { <i>unit/slot/port</i> all}
Mode	Privileged EXEC

MRP Commands

Multiple Registration Protocol (MRP) provides the same functionality as GARP, which it replaces.

MRP consist of an application and a declaration component. In addition, a distribution component is called the MRP Attribute Declaration (MAD), which transmits and processes incoming MRP Protocol Data Units (MRP PDUs). The application component keeps track of attributes via registrations, and enforces any associated rules such as attribute restrictions.

An AVB bridge such as a switch includes an MRP Attribute Propagation (MAP) component that propagates information among participating interfaces.

mrp

M4250

M4350

This command sets the MRP protocol timers on an interface.

Format	mrp {jointime <i>centiseconds</i> leavetime <i>centiseconds</i> leavealltime <i>centiseconds</i> }

Mode	Interface Config

Parameter	Description
jointime <i>centiseconds</i>	The interval between the transmission of MRP PDUs registering (or reregistering) membership for an attribute. There is an instance of this timer on a per-port, per-MRP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The default is 20 centiseconds (0.2 seconds). The finest granularity of specification is one centisecond (0.01 seconds).
leavetime <i>centiseconds</i>	The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. You can consider this a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-MRP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6 seconds). The default is 300 centiseconds (3.0 seconds).
leavealltime <i>centiseconds</i>	The LeaveAllTime controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations are shortly to be deregistered. Participants must to rejoin in order to maintain registration. There is an instance of this timer on a per-port, per-MRP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The default is 2000 centiseconds (20 seconds).

no mrp

This command sets a selected MRP protocol timer to its default value.

Format	no mrp {jointime leavetime leavealltime}

Mode	Interface Config

show mrp

M4250

M4350

This command displays MRP leave, join, and leaveall intervals configured on a specific interface or LAG, or on all interfaces. If you specify the **summary** parameter, the output shows interval values for all interfaces. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format `show mrp interface {summary | unit/slot/port | lag lag-intf-num}`

Mode Privileged Exec

Command example:

(Netgear switch) #show mrp interface summary

Intf	JoinTimer	LeaveTimer	LeaveAllTimer
-----	-----	-----	-----
0/1	20	300	2000
0/2	20	300	2000
0/3	20	300	2000
0/4	20	300	2000
0/5	20	300	2000
0/6	20	300	2000
0/7	20	300	2000
0/8	20	300	2000
0/9	20	300	2000
0/10	20	300	2000
0/11	20	300	2000
0/12	20	300	2000
lag 1	20	300	2000
lag 2	20	300	2000
lag 3	20	300	2000
lag 4	20	300	2000
lag 5	20	300	2000
lag 6	20	300	2000
lag 7	20	300	2000
lag 8	20	300	2000

MMRP Commands

Multiple MAC Registration Protocol (MMRP) propagates MAC address information in a network. MMRP replaces GMRP.

MMRP can register and deregister both individual MAC addresses and group MAC address memberships. This differs from GMRP, which supports only the propagation of group MAC address memberships.

MMRP lets end stations join or leave a multicast group or register an individual MAC address with a specific VLAN. If you enable MMRP, the switch can dynamically register and deregister MAC addresses.

mmrp (Global Config)

M4250

M4350

Use this command in Global Config mode to enable MMRP. MMRP must also be enabled on the individual interfaces.

Default	Disabled
Format	mmrp
Mode	Global Config

no mmrp (Global Config)

Use this command in Global Config mode to disable MMRP.

Format	no mmrp
Mode	Global Config

mmrp periodic state machine

M4250

M4350

Use this command in Global Config mode to enable the MMRP periodic state machine.

Default	Disabled
Format	mmrp periodic state machine
Mode	Global Config

no mmrp periodic state machine

Use this command in Global Config mode to disable the MMRP periodic state machine.

Format	no mmrp periodic state machine
Mode	Global Config

mmrp (Interface Config)

M4250

M4350

Use this command in Interface Config mode on an interface. You can enable MMRP on physical interfaces and LAG interfaces. When configured on a LAG member port, MMRP is operationally disabled. Enabling MMRP on an interface automatically enables dynamic MFDB entries creation.

Default	Disabled
Format	<code>mmrp</code>
Mode	Interface Config

no mmrp (Interface Config)

Use this command in Interface Config mode to disable MMRP on an interface.

Format	<code>no mmrp</code>
Mode	Global Config

show mmrp

M4250

M4350

Use this command in Privileged EXEC mode to display the status of the MMRP configuration. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	<code>show mmrp {summary interface {unit/slot/port lag lag-intf-num summary}}</code>
Mode	Privileged EXEC

Parameter	Description
summary	If used with the summary parameter, the command displays global MMRP information.
interface	If interface is specified for a particular <i>unit/slot/port</i> or <i>lag-intf-num</i> , the command displays the MMRP mode of that interface.
summary	If interface is specified with the summary parameter, the command shows MMRP Information for all interfaces.

Command example:

```
(NETGEAR switch) #show mmrp summary
MMRP Global Admin Mode..... Disabled
MMRP Periodic State Machine..... Disabled
```

Command example:

```
(NETGEAR switch) #show mmrp interface 0/12
MMRP Interface Admin Mode..... Disabled
```

Command example:

```
(NETGEAR switch) #show mmrp interface summary
```

Intf	Mode
0/1	Disabled
0/2	Disabled
0/3	Disabled
0/4	Disabled
0/5	Disabled
0/6	Disabled
0/7	Disabled
0/8	Disabled
0/9	Disabled
0/10	Disabled
0/11	Disabled
0/12	Disabled
lag 1	Disabled
lag 2	Disabled
lag 3	Disabled
lag 4	Disabled
lag 5	Disabled
lag 6	Disabled
lag 7	Disabled
lag 8	Disabled

show mmrp statistics

M4250

M4350

Use this command in Privileged EXEC mode to display statistical information about the MMRP PDUs sent and received on an interface or LAG, or on all interfaces. You can also display a summary of information. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.

- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format `show mmrp statistics {unit/slot/port | all | lag lag-intf-num | summary}`

Mode Privileged EXEC

The following statistics display when the **summary** keyword or *unit/slot/port* parameter is used. Using the **summary** keyword displays global statistics. The *unit/slot/port* parameter displays per-interface statistics.

Parameter	Description
MMRP messages received	Total number of MMRP messages received.
MMRP messages received with bad header	Total number of MMRP frames with bad headers received
MMRP messages received with bad format	Total number of MMRP frames with bad PDUs body formats received
MMRP messages transmitted	Total number of MMRP frames that sent
MMRP messages failed to transmit	Total number of MMRP frames that failed to be transmitted

The following statistics display when the **all** keyword is used.

Parameter	Description
Intf	The interface associated with the rest of the data in the row.
Rx	Total number of MMRP messages received.
Bad Header	Total number of MMRP frames with bad headers received
Bad Format	Total number of MMRP frames with bad PDUs body formats received
Tx	Total number of MMRP frames that sent
Tx Failed	Total number of MMRP frames that failed to be transmitted

Command example:

```
(Netgear switch) #show mmrp statistics all
```

Intf	Rx	Bad Header	Bad Format	Tx	Tx Failed
0/1	0	0	0	0	0
0/2	0	0	0	0	0
0/3	0	0	0	0	0
0/4	0	0	0	0	0
0/5	0	0	0	0	0
0/6	0	0	0	0	0

0/7	0	0	0	0	0
0/8	0	0	0	0	0
0/9	0	0	0	0	0
0/10	0	0	0	0	0
0/11	0	0	0	0	0
0/12	0	0	0	0	0
lag 1	0	0	0	0	0
lag 2	0	0	0	0	0
lag 3	0	0	0	0	0
lag 4	0	0	0	0	0
lag 5	0	0	0	0	0
lag 6	0	0	0	0	0
lag 7	0	0	0	0	0
lag 8	0	0	0	0	0

clear mmrp statistics

M4250

M4350

Use this command in Privileged EXEC mode to clear MMRP statistics of one or all interfaces. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	<code>clear mmrp statistics [<i>unit/slot/port</i> all]</code>

Mode	Privileged EXEC

Parameter	Description
unit/slot/port	The command clears MMRP statistics for the specified interface.
all	The command clears MMRP statistics for all interfaces.

MVRP Commands

Multiple VLAN Registration Protocol (MVRP) lets the switch automatically maintain dynamic VLAN registration entries and propagate the associated information over the network. This lets MVRP-aware devices to dynamically establish and update information about VLANs with active members, as well as information about the interfaces through which those members can be reached. MVRP replaces GVRP.

With MVRP, both end stations and switches can issue and revoke declarations related to VLAN membership, allowing MVRP participant to create or update a dynamic VLAN registration entry in the filtering database. Such an entry includes information about the VLAN and the interface on which it is received.

MVRP is also used by other protocols for dynamic VLAN creation over a network.

mvrp (Global Config)

M4250

M4350

Use this command in Global Configuration mode to enable MVRP. You must also enable MVRP on the individual interfaces on which you want to use MVRP.

Note: If MVRP is enabled on all devices and STP is disabled, statically created VLANs are propagated to other devices. Each device ends up with all the VLANs and connecting ports participating in all the VLANs. This may cause loops in the network.

Default	Disabled
Format	mvrp
Mode	Global Config

no mvrp (Global Config)

Use this command in Global Configuration mode to disable MVRP.

Format	no mvrp
Mode	Global Config

mvrp periodic state machine

M4250

M4350

Use this command in Global Configuration mode to enable the MVRP periodic state machine.

Default	Disabled
Format	mvrp periodic state machine
Mode	Global Config

no mvrp periodic state machine

Use this command in Global Configuration mode to disable the MVRP periodic state machine.

Format	no mvrp periodic state machine

Mode	Global Config

mvrp (Interface Config)

M4250

M4350

Use this command in Interface Configuration mode to enable MVRP on the interface, which must be configured in trunk mode or general mode. You can enable MVRP on physical interfaces or LAG interfaces. When configured on a LAG member port, MVRP is operationally disabled. Enabling MVRP on an interface automatically enables dynamic VLAN creation.

Default	Disabled

Format	mvrp

Mode	Interface Config

no mvrp (Interface Config)

Use this command in Interface Configuration mode to disable MVRP on the interface.

Format	no mvrp

Mode	Interface Config

show mvrp

M4250

M4350

Use this command in Privileged EXEC mode to display the status of the MVRP configuration. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	show mvrp {summary interface {unit/slot/port all lag lag-intf-num summary}}

Mode	Privileged EXEC

Parameter	Description
interface	If the interface is specified as <i>unit/slot/port</i> or lag <i>lag-intf-num</i> , the command shows MVRP mode information for that interface or LAG.
all	If the interface is specified with the a11 parameter, the command shows MVRP interfaces for the switch and for all interfaces.
summary	If the summary parameter is used, the command shows global MVRP information.

Command example:

```
(NETGEAR Switch) #show mvrp summary
```

```
MVRP global state..... Disabled
MVRP Periodic State Machine state..... Disabled
VLANs created via MVRP..... 20-45, 3001-3050
```

Command example:

```
(NETGEAR Switch) #show mvrp interface 0/12
```

```
MVRP interface state..... Enabled
VLANs declared..... 20-45, 3001-3050
VLANs registered..... none
```

Command example:

```
(NETGEAR Switch) #show mvrp interface all
```

```
Intf      Mode
-----
0/1       Disabled
0/2       Disabled
0/3       Disabled
0/4       Disabled
0/5       Disabled
0/6       Disabled
0/7       Disabled
0/8       Disabled
0/9       Disabled
0/10      Disabled
0/11      Disabled
0/12      Disabled
lag 1     Disabled
lag 2     Disabled
lag 3     Disabled
lag 4     Disabled
lag 5     Disabled
```

```
lag 6      Disabled
lag 7      Disabled
lag 8      Disabled
```

show mvrp statistics

M4250

M4350

Use this command in Privileged EXEC mode to display MVRP statistics. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	show mvrp statistics { <i>unit/slot/port</i> all lag <i>lag-intf-num</i> summary}
Mode	Privileged EXEC

Parameter	Description
interface	If the <i>unit/slot/port</i> or lag <i>lag-intf-num</i> is specified, the command shows MVRP statistics for that interface or LAG.
all	If used with the all parameter, the command shows a table with MVRP statistics for all interfaces on which MVRP is enabled.
summary	If used with the summary parameter, the command shows global MVRP statistics.

Command example:

```
(NETGEAR Switch) #show mvrp statistics summary
```

```
MVRP messages received..... 45
MVRP messages received with bad header..... 0
MVRP messages received with bad format..... 0
MVRP messages transmitted..... 16
MVRP messages failed to transmit..... 0
MVRP Message Queue Failures..... 0
```

Command example:

```
(NETGEAR Switch) #show mvrp statistics 0/12
```

```
Port..... 0/12
MVRP messages received..... 21
MVRP messages received with bad header..... 0
MVRP messages received with bad format..... 0
MVRP messages transmitted..... 8
```

```
MVRP messages failed to transmit..... 0
MVRP failed reservations..... 0
```

Command example:

```
(NETGEAR Switch) #show mvrp statistics all
```

Intf	Rx	BadHeader	BadFormat	Tx	Tx Failed	RegFails
-----	-----	-----	-----	-----	-----	-----
0/1	0	0	0	0	0	0
0/2	0	0	0	0	0	0
0/3	0	0	0	0	0	0
0/4	0	0	0	0	0	0
0/5	0	0	0	0	0	0
0/6	0	0	0	0	0	0
0/7	0	0	0	0	0	0
0/8	0	0	0	0	0	0
0/9	0	0	0	0	0	0
0/10	0	0	0	0	0	0
0/11	0	0	0	0	0	0
0/12	0	0	0	0	0	0
lag 1	0	0	0	0	0	0
lag 2	0	0	0	0	0	0
lag 3	0	0	0	0	0	0
lag 4	0	0	0	0	0	0
lag 5	0	0	0	0	0	0
lag 6	0	0	0	0	0	0
lag 7	0	0	0	0	0	0
lag 8	0	0	0	0	0	0

```
clear mvrp
```

M4250**M4350**

Use this command in Privileged EXEC mode to clear the MVRP statistics for one interface or LAG, or for all interfaces. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	<code>clear mvrp statistics {unit/slot/port all lag lag-intf-num}</code>
Mode	Privileged EXEC

Parameter	Description
unit/slot/port or lag lag-intf-num	If used with the <i>unit/slot/port</i> or lag <i>lag-intf-num</i> parameter, the command clears MVRP statistics for the interface or LAG.
all	If the a11 parameter is specified, the command clears MVRP statistics for all the interfaces.

MSRP Commands

Multiple Stream Reservation Protocol (MSRP) reserves resources in a network so that time-sensitive traffic can flow from end to end. A typical network includes flows for multiple talkers (devices that transmit streams) and multiple listeners (devices that receive streams from one or more talkers). Each of these flows requires a specific bandwidth, frame rate, and time synchronization. MSRP can guarantee the resources through all intermediate devices between a talker and a listener.

For example, if a particular stream requires 1000 kbps, a frame rate of 128 kbps, and not more than a maximum delay of 120 micro seconds, the requirements must be guaranteed on each device between a talker and a listener. At each bridge, the delay component is increased with the delay that is associated with that particular link. (These streams use multicast MAC addresses as directory agents [DAs] so that source pruning can occur through MMRP. Time synchronization is handled by the 802.1AS protocol, which calculates the time delay between devices on a link and maintains an accurate network clock.) The end device that receives the stream determines if the accumulated delay is within its threshold and accepts or rejects the stream.

If all devices between a talker and a listener can provide the required bandwidth and honor the minimum delay, the end device can play the stream. If a device is unable to reserve resources or contributes to an unacceptable delay, a negative acknowledgement is sent to both the talker and the listener, enabling all devices to deallocate the resources that were allocated for the stream.

MSRP ensures that the path from a talker to a listener can provide guaranteed bandwidth and timing requirement to satisfy the rigorous demands of the Ethernet audio video transmissions.

msrp (Global Config)

M4250**M4350**

Use this command in Global Configuration mode to enable MSRP. You must also enable MSRP on the individual interfaces on which you want to use MSRP.

Default	Disabled
Format	msrp
Mode	Global Config

no msrp (Global Config)

Use this command in Global Configuration mode to disable MSRP.

Format	no msrp
Mode	Global Config

msrp (Interface Config)

M4250**M4350**

Use this command in Interface Configuration mode to enable MSRP on the interface. You can enable MSRP on physical interfaces only.

Default	Disabled
Format	msrp
Mode	Interface Config

no msrp (Interface Config)

Use this command in Interface Configuration mode to disable MSRP on the interface.

Format	no msrp
Mode	Interface Config

msrp srclassqav class

M4250

M4350

This command configures Ethernet Audio/Video (EAV) traffic class mapping for class A or class B.

Default	For class A, pcp is 3 and remap is 1 For class B, pcp is 2 and remap is 1
Format	msrp srclassqav class {a {pcp remap} value b {pcp remap} value}
Mode	Global Config

Parameter	Description
pcp	Specifies the priority for the EAV traffic class in the priority code point (PCP) field.
remap	Specifies the priority for the non-EAV traffic carrying the EAV class PCP.
value	Specifies the traffic class priority, which can be a value from 0 to 7.

no msrp srclassqav class

This command sets the Ethernet Audio/Video (EAV) traffic class mapping for class A or class B to default settings.

Format	no msrp srclassqav class {a b}
Mode	Global Config

msrp boundarypropagate

M4250

M4350

This command enables MSRP boundary propagation.

Default	Disabled
Format	msrp boundarypropagate
Mode	Global Config

no msrp boundarypropagate

This command disables MSRP boundary propagation.

Format	no msrp boundarypropagate
Mode	Global Config

msrp max-fan-in-ports

M4250

M4350

This command configures the maximum number of interfaces on which MSRP registrations are allowed. The value of *number* depends on the number of ports on the switch.

Default	The default depends on the number of ports on the switch.
Format	<code>msrp max-fan-in-ports <i>number</i></code>
Mode	Global Config

no msrp max-fan-in-ports

This command sets the maximum number of interfaces on which MSRP registrations are allowed to the default value.

Format	<code>no msrp max-fan-in-ports</code>
Mode	Global Config

msrp talker-pruning

M4250

M4350

This command enables the MSRP talker-pruning feature.

Default	Disabled
Format	<code>msrp talker-pruning</code>
Mode	Global Config

no msrp talker-pruning

This command disables the MSRP talker-pruning feature.

Format	<code>no msrp talker-pruning</code>
Mode	Global Config

msrp block-avb-traffic-to-cpu

M4250**M4350**

This command blocks unknown AVB traffic from reaching the CPU. The *vlan-id* argument is the AVB VLAN ID.

Default	Disabled
Format	<code>msrp block-avb-traffic-to-cpu <i>vlan-id</i></code>
Mode	Global Config

no block-avb-traffic-to-cpu

This command unblocks unknown AVB traffic from reaching the CPU.

Format	<code>no msrp block-avb-traffic-to-cpu <i>vlan-id</i></code>
Mode	Global Config

msrp srclass-pvid

M4250**M4350**

This command configures the VLAN ID for the MSRP stream reservation (SR) traffic class on an interface. The value of *vlan-id* can be from 1 to 4093.

Default	2
Format	<code>msrp srclass-pvid <i>vlan-id</i></code>
Mode	Interface Config

no msrp srclass-pvid

This command sets the VLAN ID for the MSRP SR traffic class on an interface to the default value.

Format	<code>no msrp srclass-pvid</code>
Mode	Interface Config

msrp delta-bw

M4250**M4350**

This command configures the MSRP delta bandwidth for SR traffic class A or class B on an interface. The bandwidth *value* can be from 0 to 100.

Default	For class A, 75 For class B, 0
Format	msrp delta-bw {a <i>value</i> b <i>value</i> }
Mode	Interface Config

no msrp delta-bw

This command sets the MSRP delta bandwidth for SR traffic class A or class B for an interface to the default value.

Format	no msrp delta-bw {a b}
Mode	Interface Config

show msrp

M4250**M4350**

This command displays the status of the MSRP configuration. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	show msrp {summary interface { <i>unit/slot/port</i> lag <i>lag-intf-num</i> summary}}
Mode	Privileged EXEC

Parameter	Description
summary	If used with the summary parameter, the command displays global MSRP information.
interface	If the interface is specified as <i>unit/slot/port</i> or lag <i>lag-intf-num</i> , the command shows MSRP mode information for that interface or LAG.
summary	If interface is specified with the summary parameter, the command shows a table with MSRP information for all interfaces.

Command example:

```
(NETGEAR Switch) #show msrp summary
MSRP Global Admin Mode..... Enabled
MSRP Talker Pruning..... Disabled
MSRP Maximum Fan-in Ports..... 12
MSRP Boundary Propagation..... Disabled
QAV class A priority..... 3
QAV class A remap priority..... 1
QAV class B priority..... 2
QAV class B remap priority..... 1
```

Command example:

```
(NETGEAR Switch) #show msrp interface summary
```

Intf	Mode	SrPVID	A-Prio	A-Remap	B-Prio	B-Remap	Boundary (A / B)
0/1	Disabled	2	3	1	2	1	True / True
0/2	Disabled	2	3	1	2	1	True / True
0/3	Enabled	2	3	1	2	1	True / True
0/4	Disabled	2	3	1	2	1	True / True
0/5	Disabled	2	3	1	2	1	True / True
0/6	Disabled	2	3	1	2	1	True / True
0/7	Disabled	2	3	1	2	1	True / True
0/8	Disabled	2	3	1	2	1	True / True
0/9	Disabled	2	3	1	2	1	True / True
0/10	Disabled	2	3	1	2	1	True / True
0/11	Disabled	2	3	1	2	1	True / True
0/12	Disabled	2	3	1	2	1	True / True

show msrp interface bandwidth

M4250

M4350

This command displays the MSRP bandwidth reservation details for all interfaces.

Format	show msrp interface bandwidth
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show msrp interface bandwidth
```

Intf	Delta Bandwidth		Allocated/Total Bandwidth	
	Class A	Class B	Class A	Class B
0/1	75	0	0/0	0/0
0/2	75	0	0/0	0/0
0/3	75	0	0/0	0/0
0/4	75	0	0/0	0/0
0/5	75	0	0/937260000	0/0
0/6	75	0	0/937260000	0/0
0/7	75	0	0/0	0/0
0/8	75	0	0/0	0/0
0/9	75	0	0/937260000	0/0
0/10	75	0	0/937260000	0/0
0/11	75	0	0/0	0/0
0/12	75	0	0/0	0/0

show msrp reservations**M4250****M4350**

This command displays the MSRP stream reservation details for a specific interface or LAG. You can also specify summary or detailed information to be displayed.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format `show msrp reservations {unit/slot/port {detail | summary} | lag lag-intf-num {detail | summary} | summary}`

Mode Privileged EXEC

Command example:

```
(NETGEAR Switch) #show msrp reservations 0/10 detail
```

Stream ID	Stream MAC Address	Failure Information			Acc Latency
		Code	Intf	MAC Address	
41543	12:22:e1:65:a3:f8	0	0	00:00:00:00:00:00	647

Command example:

```
(NETGEAR Switch) #show msrp reservations 0/10 summary
```

Stream ID	Stream MAC Address	Talker Type	Listener Type	Fail Code	Information Interface	Stream Age
41543	12:22:e1:65:a3:f8	R.Adv	D.Ready	0	0	0

show msrp stream

This command displays the MSRP stream information on the switch.

Format	show msrp reservations {detail summary}

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show msrp stream detail
```

Stream ID	Stream MAC Address	Traffic Class	Stream TSpec	Failure Code	Information Intf	MAC Address	Talker Port
41543	12:22:e1:65:a3:f8	A	128 1	0 0	00:00:00:00:00:00		10

Command example:

```
(NETGEAR Switch) #show msrp stream summary
```

Stream ID	Stream MAC Address	Destination MAC Address	Acc. Latency	VLAN ID	Stream Rank
41543	12:22:e1:65:a3:f8	01:00:00:80:42:01	647	2	Regular

show msrp statistics

M4250

M4350

This command displays the MSRP statistics for the switch or for a specific interface.

Format	show msrp reservations unit/slot/port {detail summary}

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show msrp statistics 0/5

Port..... 0/5
MSRP messages received..... 0
MSRP messages received with bad header..... 0
MSRP messages received with bad format..... 0
MSRP messages transmitted..... 0
MSRP messages failed to transmit..... 0
MSRP failed registrations..... 0
```

Command example:

```
(NETGEAR Switch) #show msrp statistics summary

MSRP messages received..... 0
MSRP messages received with bad header..... 0
MSRP messages received with bad format..... 0
MSRP messages transmitted..... 0
MSRP messages failed to transmit..... 0
MSRP Message Queue Failures..... 0
```

clear msrp statistics

M4250

M4350

This command clears the MSRP statistics for one specific interface or LAG, or for all interfaces. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	clear msrp statistics [<i>unit/slot/port</i> lag <i>lag-intf-num</i> all]
Mode	Privileged EXEC

8

Routing Commands

This chapter describes the routing commands.

The chapter contains the following sections:

- [Address Resolution Protocol Commands](#)
- [IP Routing Commands](#)
- [Routing Policy Commands](#)
- [Router Discovery Protocol Commands](#)
- [Virtual LAN Routing Commands](#)
- [Virtual Router Redundancy Protocol Commands](#)
- [Virtual Router Redundancy Protocol version 3 Commands](#)
- [DHCP and BootP Relay Commands](#)
- [IP Helper Commands](#)
- [Open Shortest Path First commands](#)
- [IP Event Dampening Commands](#)
- [Routing Information Protocol Commands](#)
- [ICMP Throttling Commands](#)
- [IP Service Level Agreement Commands](#)
- [IP SLA Configuration Commands](#)

The commands in this chapter are in one of three functional groups:

- **Show commands.** Display switch settings, statistics, and other information.
- **Configuration commands.** Configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- **Clear commands.** Clear some or all of the settings to factory defaults.

Address Resolution Protocol Commands

This section describes the commands you use to configure Address Resolution Protocol (ARP) and to view ARP information on the switch. ARP associates IP addresses with MAC addresses and stores the information as ARP entries in the ARP cache.

arp

M4250

M4350

This command creates an ARP entry. The value for *ipaddress* is the IP address of a device on a subnet attached to an existing routing interface. The parameter *macaddr* is a unicast MAC address for that device. The format of the MAC address is 6 two-digit hexadecimal numbers that are separated by colons, for example 00:06:29:32:81:40

The optional *interface* parameter specifies the next hop interface or VLAN. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>arp ipaddress macaddr [interface {unit/slot/port vlan vlan-id}]</code>
Mode	Global Config

no arp

This command deletes an ARP entry. The value for *ipaddress* is the IP address of a device on a subnet attached to an existing routing interface. The parameter *macaddr* is a unicast MAC address for that device. The optional *interface* parameter specifies the next hop interface or VLAN.

Format	<code>arp ipaddress [interface {unit/slot/port vlan vlan-id}]</code>
Mode	Global Config

ip proxy-arp

M4250

M4350

This command enables proxy ARP on a router interface or range of interfaces. Without proxy ARP, a device only responds to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With proxy ARP, the device may also respond if the target IP address is reachable. The device only responds if all next hops in

its route to the destination are through interfaces other than the interface that received the ARP request.

Default	enabled
Format	<code>ip proxy-arp</code>
Mode	Interface Config

`no ip proxy-arp`

This command disables proxy ARP on a router interface.

Format	<code>no ip proxy-arp</code>
Mode	Interface Config

`ip local-proxy-arp`

M4250

M4350

Use this command to allow an interface to respond to ARP requests for IP addresses within the subnet and to forward traffic between hosts in the subnet.

Default	disabled
Format	<code>ip local-proxy-arp</code>
Mode	Interface Config

`no ip local-proxy-arp`

This command resets the local proxy ARP mode on the interface to the default value.

Format	<code>no ip local-proxy-arp</code>
Mode	Interface Config

`arp cachesize`

M4250

M4350

This command configures the ARP cache size. The ARP cache size value is a platform-specific integer value. The default size also varies depending on the platform.

Format	<code>arp cachesize <i>cache-size</i></code>
Mode	Global Config

no arp cachesize

This command configures the default ARP cache size.

Format	no arp cachesize

Mode	Global Config

arp dynamicrenew

M4250

M4350

This command enables the ARP component to automatically renew dynamic ARP entries when they age out. When an ARP entry reaches its maximum age, the system must decide whether to retain or delete the entry. If the entry has recently been used to forward data packets, the system will renew the entry by sending an ARP request to the neighbor. If the neighbor responds, the age of the ARP cache entry is reset to 0 without removing the entry from the hardware. Traffic to the host continues to be forwarded in hardware without interruption. If the entry is not being used to forward data packets, then the entry is deleted from the ARP cache, unless the dynamic renew option is enabled. If the dynamic renew option is enabled, the system sends an ARP request to renew the entry. When an entry is not renewed, it is removed from the hardware and subsequent data packets to the host trigger an ARP request. Traffic to the host may be lost until the switch receives an ARP reply from the host. Gateway entries, entries for a neighbor router, are always renewed. The dynamic renew option applies only to host entries.

The disadvantage of enabling dynamic renew is that once an ARP cache entry is created, that cache entry continues to take space in the ARP cache as long as the neighbor continues to respond to ARP requests, even if no traffic is being forwarded to the neighbor. In a network where the number of potential neighbors is greater than the ARP cache capacity, enabling dynamic renew could prevent some neighbors from communicating because the ARP cache is full.

Default	disabled

Format	arp dynamicrenew

Mode	Global Config

no arp dynamicrenew

This command prevents dynamic ARP entries from renewing when they age out.

Format	no arp dynamicrenew

Mode	Global Config

arp resptime

M4250**M4350**

This command configures the ARP request response time-out.

The value for *seconds* is a valid positive integer, which represents the IP ARP entry response time-out time in seconds. The range for *seconds* is between 1-10 seconds.

Default	1
Format	arp resptime <i>seconds</i>
Mode	Global Config

no arp resptime

This command configures the default ARP request response timeout.

Format	no arp resptime
Mode	Global Config

arp retries

M4250**M4350**

This command configures the ARP count of maximum request for retries.

The value for *retries* is an integer, which represents the maximum number of request for retries. The range for *retries* is an integer between 0-10 retries.

Default	4
Format	arp retries <i>retries</i>
Mode	Global Config

no arp retries

This command configures the default ARP count of maximum request for retries.

Format	no arp retries
Mode	Global Config

arp timeout

M4250**M4350**

This command configures the ARP entry ageout time.

The value for *seconds* is a valid positive integer, which represents the IP ARP entry ageout time in seconds. The range for *seconds* is between 15-21600 seconds.

Default	1200
Format	arp timeout <i>seconds</i>
Mode	Global Config

no arp timeout

This command configures the default ARP entry ageout time.

Format	no arp timeout
Mode	Global Config

load-interval

M4250**M4350**

This command changes the length of time for which data is used to compute load statistics. You must enter the time in seconds, and the time must be a multiple of 30, in a range from 30–600 seconds. The smaller the value of the load interval, the more accurate the instantaneous rate of the load statistics. However, a small value can affect the performance of the switch.

Default	300 seconds
Format	load-interval <i>interval</i>
Mode	Interface Config

no load-interval

This command resets the load interval on the interface to the default value.

Format	no load-interval
Mode	Interface Config

arp purge

M4250

M4350

This command causes the specified IP address to be removed from the ARP cache. Only entries of type dynamic or gateway are affected by this command.

The *ipaddr* parameter is the IP address that must be removed from the ARP cache.

The optional **interface** keyword and its associated parameters specify the interface or VLAN from which the IP address must be removed. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	arp purge <i>ipaddr</i> [interface { <i>unit/slot/port</i> <i>vlan vlan-id</i> }]
Mode	Privileged EXEC

clear arp-cache

M4250

M4350

This command causes all ARP entries of type dynamic to be removed from the ARP cache. If the **gateway** keyword is specified, the dynamic entries of type gateway are purged as well.

Format	clear arp-cache [<i>gateway</i>]
Mode	Privileged EXEC

clear arp-switch

M4250

M4350

Use this command to clear the contents of the switch's Address Resolution Protocol (ARP) table that contains entries learned through the Management port. To observe whether this command is successful, ping from the remote system to the switch. Issue the **show arp switch** command to see the ARP entries. Then issue the **clear arp-switch** command and check the **show arp switch** entries: ARP entries are no longer shown.

Format	clear arp-switch
Mode	Privileged EXEC

show arp

M4250

M4350

This command displays the Address Resolution Protocol (ARP) cache. The displayed results are not the total ARP entries. To view the total ARP entries, view the output of the **show arp** command in conjunction with the output of the **show arp switch** command.

Format	show arp
Mode	Privileged EXEC
Term	Definition
Age Time (seconds)	The time it takes for an ARP entry to age out. This is configurable. Age time is measured in seconds.
Response Time (seconds)	The time it takes for an ARP request timeout. This value is configurable. Response time is measured in seconds.
Retries	The maximum number of times an ARP request is retried. This value is configurable.
Cache Size	The maximum number of entries in the ARP table. This value is configurable.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	The total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	The static entry count in the ARP table and maximum static entry count in the ARP table.

The following are displayed for each ARP entry:

Term	Definition
IP Address	The IP address of a device on a subnet attached to an existing routing interface.
MAC Address	The hardware MAC address of that device.
Interface	The routing <i>unit/slot/port</i> associated with the device ARP entry.
Type	The type that is configurable. The possible values are Local, Gateway, Dynamic and Static.
Age	The current age of the ARP entry since last refresh (in hh:mm:ss format)

show arp brief

M4250

M4350

This command displays the brief Address Resolution Protocol (ARP) table information.

Format	show arp brief
Mode	Privileged EXEC
Term	Definition
Age Time (seconds)	The time it takes for an ARP entry to age out. This value is configurable. Age time is measured in seconds.
Response Time (seconds)	The time it takes for an ARP request timeout. This value is configurable. Response time is measured in seconds.
Retries	The maximum number of times an ARP request is retried. This value is configurable.
Cache Size	The maximum number of entries in the ARP table. This value is configurable.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	The total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	The static entry count in the ARP table and maximum static entry count in the ARP table.

show arp switch (Address Resolution Protocol commands)

This command displays the contents of the switch's Address Resolution Protocol (ARP) table.

Format	show arp switch
Mode	Privileged EXEC
Term	Definition
IP Address	The IP address of a device on a subnet attached to the switch.
MAC Address	The hardware MAC address of that device.
Interface	The routing <i>unit/slot/port</i> associated with the device's ARP entry.

IP Routing Commands

This section describes the commands you use to enable and configure IP routing on the switch.

autostate

M4250

M4350

This command enables AutoState for a VLAN routing interface. AutoState changes the state of a VLAN routing interface automatically based on link state events (up or down).

By default, AutoState is disabled, which means that a VLAN routing interface could remain up even if the link is down.

Format	autostate
Mode	Interface Config

no autostate

This command disables AutoState for a VLAN routing interface.

Format	no autostate
Mode	Interface Config

routing

M4250

M4350

This command enables IPv4 and IPv6 routing for an interface or range of interfaces. You can view the current value for this function with the **show ip brief** command. The value is labeled as Routing Mode.

Default	disabled
Format	routing
Mode	Interface Config

no routing

This command disables routing for an interface.

You can view the current value for this function with the **show ip brief** command. The value is labeled as Routing Mode.

Format	no routing

Mode	Interface Config

ip routing

M4250

M4350

This command enables the IP routing for the switch.

Format	ip routing

Mode	Global Config

no ip routing

This command disables IP routing for the switch.

Format	no ip routing

Mode	Global Config

ip address

M4250

M4350

This command configures an IP address on an interface or range of interfaces. You can also use this command to configure one or more secondary IP addresses on the interface. The command supports RFC 3021 and accepts using 31-bit prefixes on IPv4 point-to-point links. This command adds the label IP address in the command [show ip interface on page 931](#).

Note: The 31-bit subnet mask is only supported on routing interfaces. The feature is not supported on network port and service port interfaces because the switch acts as a host, not a router, on these management interfaces.

Format	<code>ip address <i>ipaddr</i> [<i>subnetmask</i> <i>/prefix-length</i>] [<i>secondary</i>]</code>
Mode	Interface Config
Parameter	Description
<i>ipaddr</i>	The IP address of the interface.
<i>subnetmask</i>	A 4-digit dotted-decimal number which represents the subnet mask of the interface.
<i>/prefix-length</i>	Implements RFC 3021. Using the / notation of the subnet mask, this is an integer that indicates the length of the subnet mask. Range is 5 to 32 bits.

Command example:

The following example configures the subnet mask with an IP address in the dotted decimal format on interface 0/4/1.

```
(NETGEAR Switch) #config
(NETGEAR Switch) (Config)#interface 0/4/1
(NETGEAR Switch) (Interface 0/4/1)#ip address 192.168.10.1 255.255.255.254
```

Command example:

The following example configures the subnet mask with an IP address in the / notation on interface 0/4/1.

```
(NETGEAR Switch) #config
(NETGEAR Switch) (Config)#interface 0/4/1
(NETGEAR Switch) (Interface 0/4/1)#ip address 192.168.10.1 /31
```

no ip address

This command deletes an IP address from an interface. The value for *ipaddr* is the IP address of the interface in a.b.c.d format where the range for a, b, c, and d is 1-255. The value for *subnetmask* is a 4-digit dotted-decimal number which represents the Subnet Mask of the interface. To remove all of the IP addresses (primary and secondary) configured on the interface, enter the command **no ip address**.

Format	<code>no ip address [<i>ipaddr</i> [<i>subnetmask</i> <i>/prefix-length</i>] [<i>secondary</i>]]</code>
Mode	Interface Config

ip address dhcp**M4250****M4350**

This command enables the DHCPv4 client on an in-band interface so that it can acquire network information, such as the IP address, subnet mask, and default gateway, from a

network DHCP server. When DHCP is enabled on the interface, the system automatically deletes all manually configured IPv4 addresses on the interface.

To enable the DHCPv4 client on an in-band interface and send DHCP client messages with the client identifier option, use the **ip address dhcp client-id** configuration command in interface configuration mode.

Default	disabled
Format	ip address dhcp [client-id]
Mode	Interface Config

Command example:

The following example enables DHCPv4 on interface 0/4/1:

```
(NETGEAR Switch) #config
(NETGEAR Switch) (Config)#interface 0/4/1
(NETGEAR Switch) (Interface 0/4/1)#ip address dhcp
```

no ip address dhcp

The **no ip address dhcp** command releases a leased address and disables DHCPv4 on an interface. The **no** form of the **ip address dhcp client-id** command removes the client-id option and also disables the DHCP client on the in-band interface.

Format	no ip address dhcp [client-id]
Mode	Interface Config

ip default-gateway

M4250

M4350

This command manually configures a default gateway for the switch. Only one default gateway can be configured. If you invoke this command multiple times, each command replaces the previous value.

When the system does not have a more specific route to a packet's destination, it sends the packet to the default gateway. The system installs a default IPv4 route with the gateway address as the next hop address. The route preference is 253. A default gateway configured with this command is more preferred than a default gateway learned from a DHCP server.

Format	ip default-gateway ipaddr
Mode	Global Config

Parameter	Description
ipaddr	The IPv4 address of an attached router.

Command example:

The following example sets the default gateway to 10.1.1.1:

```
(NETGEAR Switch) #config
(NETGEAR Switch) (Config)#ip default-gateway 10.1.1.1
```

no ip default-gateway

This command removes the default gateway address from the configuration.

Format	no ip default-gateway <i>ipaddr</i>
Mode	Interface Config

ip load-sharing

M4250

M4350

This command configures the IP equal-cost multipath (ECMP) load balancing mode.

Default	6
Format	ip load-sharing <i>mode</i> {inner outer}
Mode	Global Config

Parameter	Description
mode	1. The mode is based on a hash using the source IP address of the packet. 2. The mode is based on a hash using the destination IP address of the packet. 3. The mode is based on a hash using the source and destination IP addresses of the packet. 4. The mode is based on a hash using the source IP address and the Source TCP/UDP Port field of the packet. 5. The mode is based on a hash using the destination IP address and the Destination TCP/UDP Port field of the packet. 6. The mode is based on a hash using the source and destination IP addresses and the Source and Destination TCP/UDP Port fields of the packet.
inner	The inner IP header is used for tunneled packets.
outer	The outer IP header is used for tunneled packets.

no ip load-sharing

This command resets the IP ECMP load balancing mode to default mode (6).

Format	no ip load-sharing

Mode	Global Config

ip unnumbered gratuitous-arp accept

M4250

M4350

This command enables the switch to automatically configure static interface routes to an unnumbered peer when the switch dynamically receives gratuitous ARP messages. The switch uses the IP address of the loopback interface (see the **ip unnumbered loopback** command) as the IP address for the unnumbered peer. This behavior is enabled by default.

Format	ip unnumbered gratuitous-arp accept

Mode	Interface Config

no ip unnumbered gratuitous-arp accept

This command prevents the switch from automatically configuring static interface routes to an unnumbered peer when the switch dynamically receives gratuitous ARP messages.

Format	no ip unnumbered gratuitous-arp accept

Mode	Interface Config

ip unnumbered loopback

M4250

M4350

This command enables the switch to identify an unnumbered interface and specifies the numbered loopback interface from which the unnumbered interface can borrow an address.

The *interface-id* argument specifies the loopback interface ID from 0 to 63.

Format	ip unnumbered loopback <i>interface-id</i>

Mode	Interface Config

no ip unnumbered loopback

This removes an unnumbered interface configuration.

Format	no ip unnumbered loopback
Mode	Interface Config

release dhcp

M4250

M4350

Use this command to force the DHCPv4 client to release the leased address from a specified interface or VLAN. The DHCP client sends a DHCP Release message telling the DHCP server that it no longer needs the IP address, and that the IP address can be reassigned to another. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	release dhcp { <i>unit/slot/port</i> <i>vlan vlan-id</i> }
Mode	Privileged EXEC

renew dhcp

M4250

M4350

Use this command to force the DHCPv4 client to immediately renew an IPv4 address lease for a specified interface or VLAN. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Note: You can use this command on in-band ports and on the service or network (out-of-band) port.

Format	renew dhcp { <i>unit/slot/port</i> <i>service-port</i> <i>vlan vlan-id</i> }
Mode	Privileged EXEC

ip route

M4250

M4350

This command configures a static route. The *ipaddr* parameter is a valid IP address, and *subnetmask* is a valid subnet mask. The *nexthopip* parameter is a valid IP address of the next hop router. Specifying **Null0** as the nexthop parameter adds a static reject route. The optional *preference* parameter is an integer (value from 1 to 255) that allows you to 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, you control 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. A route with a preference of 255 cannot be used to forward traffic.

Optionally, you can also add a description and a tracking number from 1 to 128.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

For the static routes to be visible, you must perform the following steps:

- Enable IP routing globally.
- Enable IP routing for the interface.
- Confirm that the associated link is also up.

Default	preference—1
Format	<code>ip route ipaddr subnetmask {nexthopip Null0 {{interface {unit/slot/port vlan vlan-id} [nexthopip]}} [preference] [description description] [track number]</code>
Mode	Global Config

no ip route

This command deletes a single next hop to a destination static route. If you use the *nexthopip* argument, the next hop is deleted. If you use the **preference** keyword, the preference value of the static route is reset to its default. The other keywords and arguments function in a similar way.

Format	<code>no ip route ipaddr subnetmask {nexthopip Null0 {{interface {unit/slot/port vlan vlan-id} [nexthopip]}}</code>
Mode	Global Config

ip route default

M4250**M4350**

This command configures the default route. The value for *nexthopip* is a valid IP address of the next hop router. The *preference* is an integer value from 1 to 255. A route with a preference of 255 cannot be used to forward traffic. Optionally, you can also add a description and a tracking number from 1 to 128.

Default	preference—1
Format	<code>ip route default <i>nexthopip</i> [<i>preference</i>] [<i>description description</i>] [<i>track number</i>]</code>
Mode	Global Config

no ip route default

This command deletes all configured default routes. If the optional *nexthopip* parameter is designated, the specific next hop is deleted from the configured default route and if the optional preference value is designated, the preference of the configured default route is reset to its default.

Format	<code>no ip route default [<i>nexthopip</i>]</code>
Mode	Global Config

ip route distance

M4250**M4350**

This command sets the default distance (preference) for static routes. The distance can be a number in the range of 1–255. Lower route distance values are preferred when determining the best route. The **ip route** and **ip route default** commands allow you to optionally set the distance (preference) of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after invoking the **ip route distance** command.

Default	1
Format	<code>ip route distance <i>number</i></code>
Mode	Global Config

no ip route distance

This command sets the default static route preference value on the switch. Lower route preference values are preferred when determining the best route.

Format	no ip route distance

Mode	Global Config

ip route net-prototype

M4250

M4350

This command adds net prototype IPv4 routes to the hardware.

Format	ip route net-prototype <i>prefix/prefix-length nexthopip num-routes</i>

Mode	Global Config

Parameter	Definition
prefix/prefix-length	The destination network and mask for the route.
nexthopip	The next-hop IP address, which must belong to an active routing interface but does not need to be resolved.
num-routes	The number of routes that must be added to the hardware starting from the specified prefix argument and within the specified prefix length.

no ip route net-prototype

This command deletes all the net prototype IPv4 routes that were added to the hardware.

Format	no ip route net-prototype

Mode	Global Config

ip netdirbcast

M4250

M4350

This command enables the forwarding of network-directed broadcasts on an interface or range of interfaces. When enabled, network directed broadcasts are forwarded. When disabled they are dropped.

Default	disabled

Format	ip netdirbcast

Mode	Interface Config

no ip netdirbcast

This command disables the forwarding of network-directed broadcasts. When disabled, network directed broadcasts are dropped.

Format	no ip netdirbcast
Mode	Interface Config

ip prefix-list

M4250

M4350

To create a prefix list or add a prefix list entry, use the **ip prefix-list** command in Global Configuration mode. Prefix lists allow matching of route prefixes with those specified in the prefix list. Each prefix list includes a sequence of prefix list entries ordered by their sequence numbers. A router or switch sequentially examines each prefix list entry to determine if the route's prefix matches that of the entry. An empty or nonexistent prefix list permits all prefixes. An implicit deny action is assumed if a prefix does not match any entries of a prefix list. Once a match or deny occurs, the router or switch does not go through the rest of the list.

Up to 128 prefix lists may be configured. The maximum number of statements allowed in prefix list is 64.

Default	No prefix lists are configured by default. When neither the ge nor the le option is configured, the destination prefix must match the network/length exactly. If the ge option is configured without the le option, any prefix with a network mask greater than or equal to the ge value is considered a match. Similarly, if the le option is configured without the ge option, a prefix with a network mask less than or equal to the le value is considered a match.
Format	ip prefix-list <i>list-name</i> {[seq <i>number</i>] {permit deny} <i>network/length</i> [ge <i>length</i>] [le <i>length</i>] renumber [<i>renumber-interval</i>] [<i>first-statement-number</i>] }
Mode	Global Configuration

Parameter	Description
<i>list-name</i>	The text name of the prefix list. Up to 32 characters.
<i>seq number</i>	(Optional) The sequence number for this prefix list statement. Prefix list statements are ordered from lowest sequence number to highest and applied in that order. If you do not specify a sequence number, the switch automatically selects a sequence number five larger than the last sequence number in the list. Two statements may not be configured with the same sequence number. The value range for <i>number</i> is from 1 to 4,294,967,294.
permit	Permits routes for which the destination prefix matches the statement.
deny	Denies routes for which the destination prefix matches the statement.
<i>network/length</i>	Specifies the match criteria for routes being compared to the prefix list statement. The network can be any valid IP prefix. The length is any IPv4 prefix length from 0 to 32.

Parameter	Description
<i>ge length</i>	(Optional) If this option is configured, then a prefix is only considered a match if its network mask length is greater than or equal to this value. This value must be longer than the network length and less than or equal to 32.
<i>le length</i>	(Optional) If this option is configured, then a prefix is only considered a match if its network mask length is less than or equal to this value. This value must be longer than the <i>ge length</i> and less than or equal to 32.
<i>renumber</i> <i>renumber-interval</i> <i>first-statement-number</i>	(Optional) Provides the option to renumber the sequence numbers of the IP prefix list statements with a specified interval starting from a particular sequence number. The valid range for <i>renumber-interval</i> is 1–100, and the valid range for <i>first-statement-number</i> is 1–1000.

Command example:

The following example configures a prefix list that allows routes with one of two specific destination prefixes, 172.20.0.0/16 and 192.168.1.0/24:

```
(NETGEAR Switch) (config)# ip prefix-list apple seq 10 permit 172.20.0.0/16
(NETGEAR Switch) (config)# ip prefix-list apple seq 20 permit 192.168.10/24
```

Command example:

The following example disallows only the default route:

```
(NETGEAR Switch) (config)# ip prefix-list orange deny 0.0.0.0/0
(NETGEAR Switch) (config)# ip prefix-list orange permit 0.0.0.0/0 ge 1
```

no ip prefix-list

Use this command to delete a prefix list or a statement in a prefix list. The command deletes the entire prefix list. To remove an individual statement from a prefix list, you must specify the statement exactly, with all its options.

Format	no ip prefix-list <i>list-name</i> [[seq <i>number</i>] {permit deny} <i>network/length</i> [ge <i>length</i>] [le <i>length</i>]]
Mode	Global Configuration

ip prefix-list description

M4250

M4350

This command applies a text description to a prefix list.

Default	No description

Format	<code>ip prefix-list <i>list-name</i> description <i>text</i></code>

Mode	Global Configuration

Parameter	Description
<i>list-name</i>	The text name of the prefix list. Up to 32 characters.
<i>text</i>	The text description of the prefix list. You can enter up to 80 characters.

no ip prefix-list description

This command removes a text description from a prefix list.

Format	<code>no ip prefix-list <i>list-name</i></code>

Mode	Global Configuration

ip mtu

M4250

M4350

This command sets the IP Maximum Transmission Unit (MTU) on a routing interface or range of interfaces. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. Forwarded packets are dropped if they exceed the IP MTU of the outgoing interface. The MTU *size* is a number in the range 68–12270.

OSPF advertises the IP MTU in the Database Description packets it sends to its neighbors during database exchange. If two OSPF neighbors advertise different IP MTUs, they will not form an adjacency.

Note: The IP MTU size refers to the maximum size of the IP packet (IP Header + IP payload). It does not include any extra bytes that may be required for Layer-2 headers. To receive and process packets, the Ethernet MTU (see [mtu on page 483](#)) must take into account the size of the Ethernet header.

Default	1500 bytes

Format	<code>ip mtu <i>size</i></code>

Mode	Interface Config

no ip mtu

This command resets the ip mtu to the default value.

Format	no ip mtu

Mode	Interface Config

encapsulation

M4250

M4350

This command configures the link layer encapsulation type for the packet on an interface or range of interfaces. The encapsulation type can be **ethernet** or **snap**.

Default	ethernet

Format	encapsulation {ethernet snap}

Mode	Interface Config

Note: Routed frames are always ethernet encapsulated when a frame is routed to a VLAN.

show dhcp lease

M4250

M4350

This command displays a list of IPv4 addresses currently leased from a DHCP server on a specific in-band interface or all in-band interfaces. This command does not apply to service or network ports.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show dhcp lease [interface <i>unit/slot/port</i>] vlan <i>vlan-id</i>

Modes	Privileged EXEC

Term	Definition

IP address, Subnet mask	The IP address and network mask leased from the DHCP server

DHCP Lease server	The IPv4 address of the DHCP server that leased the address.

Term	Definition
State	State of the DHCPv4 Client on this interface
DHCP transaction ID	The transaction ID of the DHCPv4 Client
Lease	The time (in seconds) that the IP address was leased by the server
Renewal	The time (in seconds) when the next DHCP renew Request is sent by DHCPv4 Client to renew the leased IP address
Rebind	The time (in seconds) when the DHCP Rebind process starts
Retry count	Number of times the DHCPv4 client sends a DHCP REQUEST message before the server responds

show ip brief

M4250

M4350

This command displays all the summary information of the IP, including the ICMP rate limit configuration and the global ICMP Redirect configuration.

Format show ip brief

Modes Privileged EXEC
 User EXEC

Term	Definition
Default Time to Live	The computed TTL (Time to Live) of forwarding a packet from the local router to the final destination.
Routing Mode	Shows whether the routing mode is enabled or disabled.
Maximum Next Hops	The maximum number of next hops the packet can travel.
Maximum Routes	The maximum number of routes the packet can travel.
ICMP Rate Limit Interval	Shows how often the token bucket is initialized with burst-size tokens. Burst-interval is from 0 to 2147483647 milliseconds. The default burst-interval is 1000 msec.
ICMP Rate Limit Burst Size	Shows the number of ICMPv4 error messages that can be sent during one burst-interval. The range is from 1 to 200 messages. The default value is 100 messages.
ICMP Echo Replies	Shows whether ICMP Echo Replies are enabled or disabled.
ICMP Redirects	Shows whether ICMP Redirects are enabled or disabled.

Command example:

```
(NETGEAR Switch) #show ip brief
```

```
Default Time to Live..... 64
```

```

Routing Mode..... Disabled
Maximum Next Hops..... 4
Maximum Routes..... 128
ICMP Rate Limit Interval..... 1000 msec
ICMP Rate Limit Burst Size..... 100 messages
ICMP Echo Replies..... Enabled
ICMP Redirects..... Enabled

```

show ip dhcp client statistics

M4250

M4350

Use this command to display the client-specific DHCP statistics on all interfaces or for a specific interface.

- The **show ip dhcp client statistics** command shows the statistics on all DHCP client-enabled interfaces.
- The **show ip dhcp client statistics interface** command shows the statistics on a specific interface but only if the interface is DHCP-client enabled.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show ip dhcp client statistics [interface <i>unit/slot/port</i> vlan <i>vlan-id</i>]</code>
Modes	Privileged EXEC

Term	Definition
DHCP DISCOVER	The number of DHCP Discover packets sent by the client.
DHCP REQUEST	The number of DHCP Request packets sent by the client.
DHCP RELEASE	The number of DHCP Release packets sent by the client.
DHCP INFORM	The number of DHCP Inform packets sent by the client.
DHCP REBIND	The number of DHCP Rebind packets sent by the client.
DHCP RENEW	The number of DHCP Renew packets sent by the client.
DHCP OFFER	The number of DHCP Offer packets sent by the client.
DHCP ACK	The number of DHCP Acknowledgment packets sent by the client.
DHCP NACK	The number of DHCP Negative Acknowledgment packets sent by the client.

Command example:

```
(NETGEAR Switch)#show ip dhcp client statistics
```

```
DHCP Client Statistics for Interface 1/0/5
```

```
-----
```

Messages	Sent
-----	-----
DHCP DISCOVER.....	4
DHCP REQUEST.....	0
DHCP RELEASE.....	0
DHCP INFORM.....	0
DHCP REBIND.....	0
DHCP RENEW.....	0

Messages	Received
-----	-----
DHCP OFFER.....	0
DHCP ACK.....	0
DHCP NACK.....	0

```
DHCP Client Statistics for Interface 1/0/9
```

```
-----
```

Messages	Sent
-----	-----
DHCP DISCOVER.....	2
DHCP REQUEST.....	0
DHCP RELEASE.....	0
DHCP INFORM.....	0
DHCP REBIND.....	0
DHCP RENEW.....	0

Messages	Received
-----	-----
DHCP OFFER.....	0
DHCP ACK.....	0
DHCP NACK.....	0

Command example:

```
(NETGEAR Switch)#show ip dhcp client statistics interface 1/0/5
```

```
DHCP Client Statistics for Interface 0/5
```

```
-----

Messages                               Sent
-----                               -
DHCP DISCOVER..... 1
DHCP REQUEST..... 0
DHCP RELEASE..... 0
DHCP INFORM..... 0
DHCP REBIND..... 0
DHCP RENEW..... 0

Messages                               Received
-----                               -
DHCP OFFER..... 0
DHCP ACK..... 0
DHCP NACK..... 0
```

show ip interface

M4250

M4350

This command displays all pertinent information about the IP interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN.

The *vlan-id* is a number in the range 1–4093. The loopback *number* is in the range 0–7.

Format	show ip interface { <i>unit/slot/port</i> vlan <i>vlan-id</i> loopback <i>number</i> }
Modes	Privileged EXEC User EXEC

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Routing Interface Status	Determine the operational status of IPv4 routing Interface. The possible values are Up or Down.
Primary IP Address	The primary IP address and subnet masks for the interface. This value appears only if you configure it.
Method	Shows whether the IP address was configured manually or acquired from a DHCP server.
Secondary IP Address	One or more secondary IP addresses and subnet masks for the interface. This value appears only if you configure it.
Helper IP Address	The helper IP addresses configured by the command <code>ip helper-address</code> (Interface Config) on page 1007 .
Routing Mode	The administrative mode of router interface participation. The possible values are enable or disable. This value is configurable.
Administrative Mode	The administrative mode of the specified interface. The possible values of this field are enable or disable. This value is configurable.
Forward Net Directed Broadcasts	Displays whether forwarding of network-directed broadcasts is enabled or disabled. This value is configurable.
Proxy ARP	Displays whether Proxy ARP is enabled or disabled on the system.
Local Proxy ARP	Displays whether Local Proxy ARP is enabled or disabled on the interface.
Active State	Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.
Link Speed Data Rate	An integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).
MAC Address	The burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.
Encapsulation Type	The encapsulation type for the specified interface. The types are: Ethernet or SNAP.
IP MTU	The maximum transmission unit (MTU) size of a frame, in bytes.
Bandwidth	Shows the bandwidth of the interface.
Destination Unreachables	Displays whether ICMP Destination Unreachables may be sent (enabled or disabled).
ICMP Redirects	Displays whether ICMP Redirects may be sent (enabled or disabled).
DHCP Client Identifier	The client identifier is displayed in the output of the command only if DHCP is enabled with the client-id option on the in-band interface. See the ip address dhcp command.

Command example:

```
(NETGEAR Switch) #show ip interface 1/0/2
```

```
Routing Interface Status..... Down
Primary IP Address..... 1.2.3.4/255.255.255.0
Method..... Manual
Secondary IP Address(es)..... 21.2.3.4/255.255.255.0
..... 22.2.3.4/255.255.255.0
Helper IP Address..... 1.2.3.4
..... 1.2.3.5
Routing Mode..... Disable
Administrative Mode..... Enable
Forward Net Directed Broadcasts..... Disable
Proxy ARP..... Enable
Local Proxy ARP..... Disable
Active State..... Inactive
Link Speed Data Rate..... Inactive
MAC Address..... 00:10:18:82:0C:68
Encapsulation Type..... Ethernet
IP MTU..... 1500
Bandwidth..... 100000 kbps
Destination Unreachables..... Enabled
ICMP Redirects..... Enabled
```

Command example:

The following example enables the DHCP client on a VLAN routing interface:

```
(NETGEAR Switch) #show ip interface vlan 10
```

```
Routing Interface Status..... Up
Method..... DHCP
Routing Mode..... Enable
Administrative Mode..... Enable
Forward Net Directed Broadcasts..... Disable
Active State..... Inactive
Link Speed Data Rate..... 10 Half
MAC address..... 00:10:18:82:16:0E
Encapsulation Type..... Ethernet
IP MTU..... 1500
Bandwidth..... 10000 kbps
Destination Unreachables..... Enabled
ICMP Redirects..... Enabled
Interface Suppress Status..... Unsuppressed
DHCP Client Identifier..... ONETGEAR-0010.1882.160E-v110
```

show ip interface brief

M4250**M4350**

This command displays summary information about IP configuration settings for all ports on the switch, and indicates how each IP address was assigned.

Format	show ip interface brief
Modes	Privileged EXEC User EXEC
Term	Definition
Interface	Valid unit and port number separated by a forward slash.
State	Routing operational state of the interface.
IP Address	The IP address of the routing interface in 32-bit dotted decimal format.
IP Mask	The IP mask of the routing interface in 32-bit dotted decimal format.
Method	Indicates how each IP address was assigned. The field contains one of the following values: - DHCP. The address is leased from a DHCP server. - Manual. The address is manually configured.

Command example:

```
(alpha1) #show ip interface brief
```

Interface	State	IP Address	IP Mask	Method
1/0/17	Up	192.168.75.1	255.255.255.0	DHCP

show ip load-sharing

M4250**M4350**

This command displays the configured IP ECMP load balancing mode.

Format	show ip load-sharing
Mode	Privileged Exec

Command example:

```
(NETGEAR Switch) #show ip load-sharing
ip load-sharing 6 inner
```

show ip protocols

M4250**M4350**

This command lists a summary of the configuration and status for each unicast routing protocol that is running. The command lists routing protocols that are configured and enabled. If you specify a protocol, the command output is limited to the protocol.

Format	show ip protocols [rip]
Mode	Privileged Exec
Term	Description
RIP Admin Mode	Whether RIP is globally enabled.
Split Horizon Mode	Whether RIP advertises routes on the interface on which the routes are received.
Default Metric	The metric assigned to redistributed routes.
Default Route Advertise	Whether the switch is originating a default route.
Distance	The administrative distance for RIP routes.
Redistribution	A table showing information for each source protocol (connected and static). For each of these sources, the distribution list and metric are shown. Fields that are not configured are left blank.
Interface	The interfaces on which RIP is enabled and the version that is sent and accepted on each interface.

Command example:

```

Routing Protocol..... RIP
RIP Admin Mode..... Enable
Split Horizon Mode..... Simple
Default Metric..... Not configured
Default Route Advertise..... Disable
Distance..... 120
Redistribution:
Source    Metric Dist List Match
-----
connected      6
static         10      15
Interface              Send      Recv
-----
0/25                 RIPv2      RIPv2

```

show ip route

M4250

M4350

This command displays the routing table. The *ip-address* specifies the network for which the route is to be displayed and displays the best matching best-route for the address. The *mask* specifies the subnet mask for **the specified** *ip-address*. When you use the **longer-prefixes** keyword, the *ip-address* and *mask* pair becomes the prefix, and the command displays the routes to the addresses that match that prefix. Use the *protocol* parameter to specify the protocol that installed the routes. The value for *protocol* can be **connected**, **rip**, or **static**. For an M4350 series switch, **ospf** is also supported.

Use the optional **all** parameter to display all routes including best and non-best routes. If you do not use the **all** parameter, the command displays only the best route.

Note: If you use the **connected** keyword for *protocol*, the **all** option is not available because there are no best or non-best connected routes.

Note: If you use the **static** keyword for *protocol*, the *description* option is also available, for example: **show ip route ip-address static description**. This command shows the description configured with the specified static route(s).

Format	<code>show ip route [{ip-address [protocol] ip-address mask [longer-prefixes] [protocol] protocol}] [all]</code>

Modes	Privileged EXEC User EXEC

Term	Definition
Route Codes	The key for the routing protocol codes that might appear in the routing table output.

The **show ip route** command displays the routing tables in the following format:

```
Code  IP-Address/Mask [Preference/Metric] via Next-Hop, Route-Timestamp, Interface,
Truncated
```

The columns for the routing table display the following information:

Term	Definition
Code	The codes for the routing protocols that created the routes.
Default Gateway	The IP address of the default gateway. When the system does not have a more specific route to a packet's destination, it sends the packet to the default gateway.

Term	Definition
IP-Address/Mask	The IP-Address and mask of the destination network corresponding to this route.
Preference	The administrative distance associated with this route. Routes with low values are preferred over routes with higher values.
Metric	The cost associated with this route.
via Next-Hop	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.
Route-Timestamp	The last updated time for dynamic routes. The format of Route-Timestamp will be Days:Hours:Minutes if days > = 1 Hours:Minutes:Seconds if days < 1
Interface	The outgoing router interface to use when forwarding traffic to the next destination. For reject routes, the next hop interface would be Null0 interface.
T	A flag appended to a route to indicate that it is an ECMP route, but only one of its next hops has been installed in the forwarding table. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop. Such truncated routes are identified by a T after the interface name.

To administratively control the traffic destined to a particular network and prevent it from being forwarded through the switch, you can configure a static reject route on the switch. Such traffic would be discarded and the ICMP destination unreachable message is sent back to the source. This is typically used for preventing routing loops.

Command example:

```
(NETGEAR Switch) #show ip route
```

```
Route Codes: R - RIP Derived, C - Connected, S - Static
```

```
Default gateway is 1.1.1.2
C 1.1.1.0/24 [0/1] directly connected, 0/11
C 2.2.2.0/24 [0/1] directly connected, 0/1
C 5.5.5.0/24 [0/1] directly connected, 0/5
S 7.0.0.0/8 [1/0] directly connected, Null0
C 11.11.11.0/24 [0/1] directly connected, 0/11
S 12.0.0.0/8 [5/0] directly connected, Null0
S 23.0.0.0/8 [3/0] directly connected, Null0
C 1.1.1.0/24 [0/1] directly connected, 0/11
C 2.2.2.0/24 [0/1] directly connected, 0/1
C 5.5.5.0/24 [0/1] directly connected, 0/5
C 11.11.11.0/24 [0/1] directly connected, 0/11
S 10.3.2.0/24 [1/0] via 1.1.1.2, 0/11
```

show ip route ecmp-groups

M4250**M4350**

This command reports all current ECMP groups in the IPv4 routing table. An ECMP group is a set of two or more next hops used in one or more routes. The groups are numbered arbitrarily from 1 to n. The output indicates the number of next hops in the group and the number of routes that use the set of next hops. The output lists the IPv4 address and outgoing interface of each next hop in each group.

Format	show ip route ecmp-groups
Mode	Privileged Exec

Command example:

```
(NETGEAR Switch) #show ip route ecmp-groups
```

```
ECMP Group 1 with 2 next hops (used by 1 route)
```

```
  172.20.33.100 on interface 2/33
```

```
  172.20.34.100 on interface 2/34
```

```
ECMP Group 2 with 3 next hops (used by 1 route)
```

```
  172.20.32.100 on interface 2/32
```

```
  172.20.33.100 on interface 2/33
```

```
  172.20.34.100 on interface 2/34
```

```
ECMP Group 3 with 4 next hops (used by 1 route)
```

```
  172.20.31.100 on interface 2/31
```

```
  172.20.32.100 on interface 2/32
```

```
  172.20.33.100 on interface 2/33
```

```
  172.20.34.100 on interface 2/34
```

show ip route hw-failure

M4250**M4350**

This command displays the routes that were not added to the hardware because of hash errors or because the table was full.

Format	show ip route hw-failure
Mode	Privileged Exec

Command example:

```
(NETGEAR Switch) #show ip route hw-failure
```

```
Route Codes: R - RIP Derived, C - Connected, S - Static
```

```
K - Kernel, P - Net Prototype
```

```
P      66.6.6.0/24 [1/1] via 9.0.0.2,    01d:22h:15m,  0/1  hw-failure
```



```
P      66.6.7.0/24 [1/1] via 9.0.0.2,    01d:22h:15m,  0/1  hw-failure
P      66.6.8.0/24 [1/1] via 9.0.0.2,    01d:22h:15m,  0/1  hw-failure
P      66.6.9.0/24 [1/1] via 9.0.0.2,    01d:22h:15m,  0/1  hw-failure
```

show ip route kernel

M4250

M4350

A kernel route is a special route that can be configured into the Linux kernel, for example, through the Linux shell. The command output marks such a route with a K to denote that the route is installed in the kernel.

Use the optional **a11** parameter to display all routes including best and nonbest routes. If you do not use the **a11** parameter, the command displays only the best route.

Format	show ip route kernel [all]

Mode	Privileged Exec

Command example:

```
(NETGEAR Switch) #show ip route kernel
Route Codes: C - Connected, S - Static R - RIP Derived
K - Kernel, P - Net Prototype
Default Gateway(s): 172.26.2.1
```

show ip route net-prototype

M4250

M4350

This command displays the net prototype routes. The output of the command displays the net prototype routes with a P.

Format	show ip route net-p

Mode	Privileged Exec

Command example:

```
(NETGEAR Switch) #show ip route net-prototype
Route Codes: R - RIP Derived, C - Connected, S - Static,
K - Kernel, P - Net Prototype
P      56.6.6.0/24 [1/1] via 9.0.0.2,    01d:22h:15m,  0/1
P      56.6.7.0/24 [1/1] via 9.0.0.2,    01d:22h:15m,  0/1
```

show ip route summary

M4250

M4350

This command displays a summary of the state of the routing table. When the optional `all` keyword is specified, some statistics, such as the number of routes from each source, include counts for alternate routes. An alternate route is a route that is not the most preferred route to its destination and therefore is not installed in the forwarding table. To include only the number of best routes, do not use the optional keyword.

Format	<code>show ip route summary [all]</code>
Modes	Privileged EXEC User EXEC
Term	Definition
Connected Routes	The total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
RIP Routes	Total number of routes installed by RIP protocol.
Reject Routes	Total number of reject routes installed by all protocols.
Net Prototype Routes	The number of net prototype routes.
Total Routes	Total number of routes in the routing table.
Best Routes (High)	The number of best routes currently in the routing table. This number only counts the best route to each destination. The value in parentheses indicates the highest count of unique best routes since counters were last cleared.
Alternate Routes	The number of alternate routes currently in the routing table. An alternate route is a route that was not selected as the best route to its destination.
Route Adds	The number of routes that have been added to the routing table.
Route Modifies	The number of routes that have been changed after they were initially added to the routing table.
Route Deletes	The number of routes that have been deleted from the routing table.
Unresolved Route Adds	The number of route adds that failed because none of the route's next hops were on a local subnet. Note that static routes can fail to be added to the routing table at startup because the routing interfaces are not yet up. In such a situation, the counter is incremented. The static routes are added to the routing table when the routing interfaces come up.
Invalid Route Adds	The number of routes that failed to be added to the routing table because the route was invalid. A log message is written for each of these failures.
Failed Route Adds	The number of routes that failed to be added to the routing table because of a resource limitation in the routing table.
Hardware Failed Route Adds	The number of routes that failed to be inserted into the hardware because of a hash error or a table-full condition.

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Reserved Locals	The number of routing table entries reserved for a local subnet on a routing interface that is down. Space for local routes is always reserved so that local routes can be installed when a routing interface bounces.
Unique Next Hops (High)	The number of distinct next hops used among all routes currently in the routing table. These include local interfaces for local routes and neighbors for indirect routes. The value in parentheses indicates the highest count of unique next hops since counters were last cleared.
Next Hop Groups (High)	The current number of next hop groups in use by one or more routes. Each next hop group includes one or more next hops. The value in parentheses indicates the highest count of next hop groups since counters were last cleared.
ECMP Groups (High)	The number of next hop groups with multiple next hops. The value in parentheses indicates the highest count of next hop groups since counters were last cleared.
ECMP Groups	The number of next hop groups with multiple next hops.
ECMP Routes	The number of routes with multiple next hops currently in the routing table.
Truncated ECMP Routes	The number of ECMP routes that are currently installed in the forwarding table with just one next hop. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop.
ECMP Retries	The number of ECMP routes that have been installed in the forwarding table after initially being installed with a single next hop.
Routes with n Next Hops	The current number of routes with each number of next hops.

Command example:

```
(NETGEAR Switch) #show ip route summary
Connected Routes..... 7
Static Routes..... 1
RIP Routes..... 20
Reject Routes..... 0
Total routes..... 1032

Best Routes (High)..... 1032 (1032)
Alternate Routes..... 0
Route Adds..... 1010
Route Modifies..... 1
Route Deletes..... 10
Unresolved Route Adds..... 0
Invalid Route Adds..... 0
Failed Route Adds..... 0
Reserved Locals..... 0

Unique Next Hops (High)..... 13 (13)
Next Hop Groups (High)..... 13 (14)
ECMP Groups (High)..... 2 (3)
```

```

ECMP Routes..... 1001
Truncated ECMP Routes..... 0
ECMP Retries..... 0
Routes with 1 Next Hop..... 31
Routes with 2 Next Hops..... 1
Routes with 4 Next Hops..... 1000

```

clear ip route (M4250 series switch)

M4250

This command lets you reset the IPv4 routing table counters or remove various types of routes in the IPv4 routing table.

Format	<code>clear ip route {all counters rip [<i>ip-address subnet-mask</i> [interface slot/port]]}</code>
Mode	Privileged EXEC
Term	Definition
all	Removes all dynamic routes from the IPv4 routing table. Static routes are not removed.
counters	The command resets the IPv4 routing table counters to zero. These are the IPv4 routing table counters that display in the output of the show ip route summary command (see show ip route summary on page 940). The command resets event counters only. Counters that display in the current state of the routing table, such as the number of routes of each type, are not reset.
rip	Removes all RIP routes from the IPv4 routing table. By using the <i>ip-address</i> and <i>subnet-mask</i> parameters you can remove specific RIP routes. In addition, you can remove specific RIP routes from specific next hop interfaces by using the interface option and <i>slot/port</i> parameter.

clear ip route (M4350 series switch)

M4350

This command lets you reset the IPv4 routing table counters or remove various types of routes in the IPv4 routing table.

Format	<code>clear ip route {all counters ospf [<i>ip-address subnet-mask</i> [interface unit/slot/port]] rip [<i>ip-address subnet-mask</i> [interface unit/slot/port]]}</code>
Mode	Privileged EXEC
Term	Definition
all	Removes all dynamic routes from the IPv4 routing table. Static routes are not removed.
counters	The command resets the IPv4 routing table counters to zero. These are the IPv4 routing table counters that display in the output of the show ip route summary command (see show ip route summary on page 940). The command resets event counters only. Counters that display in the current state of the routing table, such as the number of routes of each type, are not reset.

Term	Definition
ospf	Removes all OSPF routes from the IPv4 routing table. By using the <i>ip-address</i> and <i>subnet-mask</i> parameters you can remove specific OSPF routes. In addition, you can remove specific OSPF routes from specific next hop interfaces by using the interface option and <i>unit/slot/port</i> parameter.
rip	Removes all RIP routes from the IPv4 routing table. By using the <i>ip-address</i> and <i>subnet-mask</i> parameters you can remove specific RIP routes. In addition, you can remove specific RIP routes from specific next hop interfaces by using the interface option and <i>unit/slot/port</i> parameter.

show ip route preferences

M4250

M4350

This command displays detailed information about the route preferences for each type of route. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values. A route with a preference of 255 cannot be used to forward traffic.

Format	show ip route preferences

Modes	Privileged EXEC User EXEC

Term	Definition
Local	The local route preference value.
Static	The static route preference value.
RIP	The RIP route preference value.
Configured Default Gateway	The route preference value of the statically-configured default gateway
DHCP Default Gateway	The route preference value of the default gateway learned from the DHCP server.

Command example:

```
(NETGEAR Switch) #show ip route preferences
```

```
Local..... 0
Static..... 1
RIP..... 120
Configured Default Gateway..... 253
DHCP Default Gateway..... 254
```

show ip prefix-list

M4250

M4350

This command displays configuration and status for a specific IPv4 prefix list.

Format `show ip prefix-list {listname [prefix/length [longer | first-match]] | listname seq 1-4294967294 | detail [listname] | summary [listname]}`

Mode Privileged Exec

Parameter	Description
<i>listname</i>	The name of the prefix list.
<i>prefix-length</i>	The IPv4 network number and length (in bits) of the network mask in the a.b.c.d/len format.
<i>first-match</i>	Displays the entry of a prefix list that matches the specified network and length.
<i>longer</i>	Displays all entries of a prefix list that are more specific than the specified network and length.
<i>seq sequence-number</i>	The sequence number for the prefix list.
<i>detail</i>	Displays detailed information about all prefix lists.
<i>summary</i>	Displays summarized information about all prefix lists.

The command output includes the following information.

Field	Description
Count	The number of entries in the prefix list.
Range Entries	The number of entries that match the input range.
Ref Count	The number of entries that reference the prefix list.
Seq	The sequence number of the entry in the prefix list.
Permit/Deny	The permit or deny action that is taken.
Sequences	The range of sequence numbers for the entries in the prefix list,
Hit Count	The number of matches for the prefix list.

Command example:

```
(NETGEAR Switch)#show ipv6 prefix-list fred
(Routing) #show ip prefix-list fred
```

```
ip prefix-list fred:
  count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
  seq 5 permit 10.10.1.1/20 ge 22
  seq 10 permit 10.10.1.2/20 le 30
```

```
seq 15 permit 10.10.1.2/20 ge 29 le 30
```

Command example:

```
(NETGEAR Switch)#show ip prefix-list summary fred
```

```
ip prefix-list fred:
```

```
count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
```

Command example:

```
(NETGEAR Switch)#show ip prefix-list detail fred
```

```
ip prefix-list fred:
```

```
count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
```

```
seq 5 permit 10.10.1.1/20 ge 22 (hitcount: 0)
```

```
seq 10 permit 10.10.1.2/20 le 30 (hitcount: 0)
```

```
seq 15 permit 10.10.1.2/20 ge 29 le 30 (hitcount: 0)
```

show ip stats**M4250****M4350**

This command displays IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed.

Format	show ip stats
Modes	Privileged EXEC User EXEC

show routing heap summary**M4250****M4350**

This command displays a summary of the memory allocation from the routing heap. The routing heap is a chunk of memory set aside when the system boots for use by the routing applications.

Format	show routing heap summary
Mode	Privileged Exec

Parameter	Description
Heap Size	The amount of memory, in bytes, allocated at startup for the routing heap.
Memory In Use	The number of bytes currently allocated.
Memory on Free List	The number of bytes currently on the free list. When a chunk of memory from the routing heap is freed, it is placed on a free list for future reuse.
Memory Available in Heap	The number of bytes in the original heap that have never been allocated.
In Use High Water Mark	The maximum memory in use since the system last rebooted.

Command example:

```
(NETGEAR Switch) #show routing heap summary
```

```
Heap Size..... 95053184
Memory In Use..... 56998
Memory on Free List..... 47
Memory Available in Heap..... 94996170
In Use High Water Mark..... 57045
```

Routing Policy Commands

ip policy route-map

M4250

M4350

Use this command to identify a route map to use for policy-based routing on an interface specified by *route-map-name*. Policy-based routing is configured on the interface that *receives* the packets, not on the interface from which the packets are sent.

When a route-map applied on the interface is changed, that is, if new statements are added to route-map or match/set terms are added/removed from route-map statement, and also if route-map that is applied on an interface is removed, route-map needs to be removed from interface and added back again in order to have changed route-map configuration to be effective.

Note: Route-map and Diffserv cannot work on the same interface.

Format	<code>ip policy route-map-name</code>

Mode	Interface Config

```
(NETGEAR Switch) (Config)#interface 1/0/1
(NETGEAR Switch) (Interface 1/0/1)#
(NETGEAR Switch) (Interface 1/0/1)# #ip policy route-map equal-access
```

no ip policy route-map

Use this command to disable policy-based routing on an interface.

Format	<code>no ip policy route-map-name</code>

Mode	Interface Config

route-map

M4250

M4350

To create a route map and enter Route Map Configuration mode, use the **route-map** command in Global Configuration mode. One use of a route map is to limit the redistribution of routes to a specified range of route prefixes. The redistribution command specifies a route map which refers to a prefix list. The prefix list identifies the prefixes that may be redistributed. The switch accepts up to 64 route maps.

Default	No route maps are configured by default. If no permit or deny tag is specified, permit is the default.

Format	<code>route-map map-tag [permit deny] [sequence-number]</code>

Mode	Global Configuration

Parameter	Description
map-tag	Text name of the route map. Route maps with the same name are grouped together in order of their sequence numbers. A route map name may be up to 32 characters long.
permit	(Optional) Permit routes that match all of the match conditions in the route map.
deny	(Optional) Deny routes that match all of the match conditions in the route map.
sequence-number	(Optional) An integer used to order the set of route maps with the same name. Route maps are ordered from lowest to greatest sequence number, with lower sequence numbers being considered first. If no sequence number is specified, the system assigns a value ten greater than the last statement in the route map. The range is 0 to 65,535.

Command example:

The following example configures BGP to redistribute all prefixes within 172.20.0.0 and reject all others:

```
(NETGEAR Switch) (config)# ip prefix-list redist-pl permit 172.20.0.0/16 le 32
(NETGEAR Switch) (config)# route-map redist-rm permit
(NETGEAR Switch) (config-route-map)# match ip address prefix-list redist-pl
(NETGEAR Switch) (config-route-map)# exit
```

no route-map

To delete a route map or one of its statements, use the **no route-map** command.

Format	no route-map <i>map-tag</i> [permit deny] [<i>sequence-number</i>]

Mode	Global Configuration

match ip address {access-list-number | access-list-name}

M4250

M4350

Use this command to configure a route map in order to match based on the match criteria configured in an IP access-list. Note that an IP ACL must be configured before it is linked to a route-map. Actions present in an IP ACL configuration are applied with other actions involved in route-map. If an IP ACL referenced by a route-map is removed or rules are added or deleted from that ACL, the configuration is rejected.

If there are a list of IP access-lists specified in this command and the packet matches at least one of these access-list match criteria, the corresponding set of actions in route-map are applied to packet.

If there are duplicate IP access-list numbers/names in this command, the duplicate configuration is ignored.

Default	No match criteria are defined by default.

Format	match ip address { <i>access-list-number</i> <i>access-list-name</i> } [... <i>access-list-number</i> <i>access-list-name</i>]

Mode	Route Map Configuration

Parameter	Description
access-list-number	The access-list number that identifies an access-list configured through access-list CLI configuration commands. This number is 1 to 99 for standard access list number. This number is 100 to 199 for extended access list number.
access-list-name	The access-list name that identifies named IP ACLs. Access-list name can be up to 31 characters in length. A maximum of 16 ACLs can be specified in this match clause.

Command example:

The following example creates a route-map with a match clause on ACL number and applies that route-map on an interface:

```
(NETGEAR Switch) (config)#access-list 1 permit ip 10.1.0.0 0.0.255.255
(NETGEAR Switch) (config)#access-list 2 permit ip 10.2.0.0 0.0.255.255
(NETGEAR Switch) (config)#route-map equal-access permit 10
(NETGEAR Switch) (config-route-map)#match ip address 1
(NETGEAR Switch) (config-route-map)#set ip default next-hop 192.168.6.6
(NETGEAR Switch) (config-route-map)#route-map equal-access permit 20
(NETGEAR Switch) (config-route-map)#match ip address 2
(NETGEAR Switch) (config-route-map)#set ip default next-hop 172.16.7.7
(NETGEAR Switch) (config)#interface 1/0/1
(NETGEAR Switch) (Interface 1/0/1)#ip address 10.1.1.1 255.255.255.0
(NETGEAR Switch) (Interface 1/0/1)#ip policy route-map equal-access
(NETGEAR Switch) (config)#interface 1/0/2
(NETGEAR Switch) (Interface 1/0/2)#ip address 192.168.6.5 255.255.255.0
(NETGEAR Switch) (config)#interface 1/0/3
(NETGEAR Switch) (Interface 1/0/3)#ip address 172.16.7.6 255.255.255.0
```

The **ip policy route-map equal-access** command is applied to interface 1/0/1. All packets coming inside 1/0/1 are policy-routed.

Sequence number 10 in route map equal-access is used to match all packets sourced from any host in subnet 10.1.0.0. If there is a match, and if the switch has no explicit route for the packet's destination, it is sent to next-hop address 192.168.6.6.

Sequence number 20 in route map equal-access is used to match all packets sourced from any host in subnet 10.2.0.0. If there is a match, and if the switch has no explicit route for the packet's destination, it is sent to next-hop address 172.16.7.7.

All other packets are forwarded as per normal L3 destination-based routing.

Command example:

The following example shows a scenario in which an IP ACL that is referenced by a route-map is removed or rules are added or deleted from that ACL:

```
(NETGEAR Switch) #show ip access-lists
```

```
Current number of ACLs: 9 Maximum number of ACLs: 100
```

ACL ID/Name	Rules	Direction	Interface(s)	VLAN(s)
1	1			
2	1			
3	1			
4	1			
5	1			
madan	1			

Fully Managed Switches M4250 and M4350 Series

```
(NETGEAR Switch) #show mac access-lists
```

```
Current number of all ACLs: 9 Maximum number of all ACLs: 100
```

MAC ACL Name	Rules	Direction	Interface(s)	VLAN(s)
-----	-----	-----	-----	-----
madan	1			
mohan	1			
goud	1			

```
(NETGEAR Switch) #
```

```
(NETGEAR Switch) #configure
```

```
(NETGEAR Switch) (Config)#route-map madan
```

```
(NETGEAR Switch) (route-map)#match ip address 1 2 3 4 5 madan
```

```
(NETGEAR Switch) (route-map)#match mac-list madan mohan goud
```

```
(NETGEAR Switch) (route-map)#exit
```

```
(NETGEAR Switch) (Config)#exit
```

```
(NETGEAR Switch) #show route-map
```

```
route-map madan permit 10
```

```
Match clauses:
```

```
ip address (access-lists) : 1 2 3 4 5 madan
```

```
mac-list (access-lists) : madan mohan goud
```

```
Set clauses:
```

```
(NETGEAR Switch) (Config)#access-list 2 permit every
```

```
Request denied. Another application using this ACL restricts the number of rules allowed.
```

```
(NETGEAR Switch) (Config)#ip access-list madan
```

```
(NETGEAR Switch) (Config-ipv4-acl)#permit udp any any
```

```
Request denied. Another application using this ACL restricts the number of rules allowed.
```

no match ip address (for an access list)

To delete a match statement for an access list from a route map, use the **no match ip address** command.

Format	no match ip address [<i>access-list-number</i> <i>access-list-name</i>]

Mode	Route Map Configuration

match length

M4250

M4350

Use this command to configure a route map to match based on the Layer 3 packet length between specified minimum and maximum values. *min* specifies the packet's minimum

Layer 3 length, inclusive, allowed for a match. *max* specifies the packet's maximum Layer 3 length, inclusive, allowed for a match. Each route-map statement can contain one 'match' statement on packet length range.

Default	No match criteria are defined by default.
Format	<code>match length <i>min max</i></code>
Mode	Route Map Configuration

Command example:

```
(NETGEAR Switch) (config-route-map)# match length 64 1500
```

no match length

Use this command to delete a match statement from a route map.

Format	<code>no match length</code>
Mode	Route Map Configuration

match mac-list

M4250

M4350

Use this command to configure a route map in order to match based on the match criteria configured in an MAC access-list.

A MAC ACL is configured before it is linked to a route-map. Actions present in the MAC ACL configuration are applied with other actions involved in the route map. When a MAC ACL referenced by a route map is removed, the route map rule is also removed and the corresponding rule is not effective. When a MAC ACL referenced by a route map is removed or rules are added or deleted from that ACL, the configuration is rejected.

You can add up to 16 MAC ACLs.

Default	No match criteria are defined by default.
Format	<code>match mac-list <i>mac-list-name</i> [<i>mac-list-name</i>]</code>
Mode	Route Map Configuration

Parameter	Description
mac-list-name	The mac-list name that identifies MAC ACLs. MAC access list name can be up to 31 characters in length.

Command example:

```
(NETGEAR Switch) (config-route-map)# match mac-list MacList1
```

Example 2:

This example illustrates the scenario where MAC ACL referenced by a route-map is removed or rules are added or deleted from that ACL, this is how configuration is rejected:

```
(NETGEAR Switch) #show mac access-lists
```

```
Current number of all ACLs: 9 Maximum number of all ACLs: 100
```

MAC ACL Name	Rules	Direction	Interface(s)	VLAN(s)
-----	----	-----	-----	-----
madan	1			
mohan	1			
goud	1			

```
(NETGEAR Switch) #
(NETGEAR Switch) #configure
(NETGEAR Switch) (Config)#route-map madan
(NETGEAR Switch) (route-map)#match mac-list madan mohan goud
(NETGEAR Switch) (route-map)#exit
(NETGEAR Switch) (Config)#exit
(NETGEAR Switch) #show route-map
```

```
route-map madan permit 10
  Match clauses:
    mac-list (access-lists) : madan mohan goud
  Set clauses:
```

```
(NETGEAR Switch) (Config)#mac access-list extended madan
(NETGEAR Switch) (Config-mac-access-list)#permit 00:00:00:00:00:01 ff:ff:ff:ff:ff:ff any
Request denied. Another application using this ACL restricts the number of rules allowed.
```

no match mac-list

To delete a match statement from a route map, use the **no match mac-list** command.

Format	no match mac-list [...mac-list-name]

Mode	Route Map Configuration

match metric

M4250

M4350

This command configures a route-metric match attribute for OSPF traffic. The *value* argument is a value from 0 to 4,294,967,295.

Default	No match criteria are defined by default.
Format	<code>match metric value</code>
Mode	Route Map Configuration

no match metric

Use this command to remove a route-metric match attribute for OSPF traffic.

Format	<code>no match metric value</code>
Mode	Route Map Configuration

match metric-type

M4250

M4350

This command configures a route-metric type match attribute for OSPF traffic. The *value* argument can be 1 or 2, which specifies external LSA metric type 1 or type 2 in OSPF.

Default	No match criteria are defined by default.
Format	<code>match metric-type value</code>
Mode	Route Map Configuration

no match metric-type

Use this command to remove a route-metric type match attribute (LSA metric type 1 or type 2) for OSPF traffic.

Format	<code>no match metric-type value</code>
Mode	Route Map Configuration

match tag

M4250

M4350

This command configures a route tag value match attribute for an external LSA route in OSPF traffic. The *value* argument can be from 0 to 4,294,967,295.

Default	No match criteria are defined by default.
Format	<code>match tag value</code>
Mode	Route Map Configuration

no match tag

Use this command to remove a route tag value match attribute for OSPF traffic.

Format	<code>no match tag value</code>
Mode	Route Map Configuration

set interface

M4250

M4350

If you do not want to revert to normal forwarding but instead want to drop a packet that does not match the specified criteria, a set statement must be configured to route the packets to interface null 0 as the last entry in the route-map. A **set interface null0** command must be configured in a separate statement. It must not be added along with any other statement that has other match or set terms.

A route map statement that is used for policy-based routing (PBR) is configured as permit or deny. If the statement is marked as deny, traditional destination-based routing is performed on the packet meeting the match criteria. If the statement is marked as permit, and if the packet meets all the match criteria, then set commands in the route-map statement are applied. If no match is found in the route map, the packet is not dropped, instead the packet is forwarded using the routing decision taken by performing destination-based routing.

Format	<code>set interface null0</code>
Mode	Route Map Configuration

no set interface

Use this command to remove interface null 0 as the last entry in the route map.

Format	no set interface null0

Mode	Route Map Configuration

set ip next-hop

M4250

M4350

Use this command to specify the adjacent next-hop router in the path toward the destination to which the packets should be forwarded. If more than one IP address is specified, the first IP address associated with a currently up-connected interface is used to route the packets.

This command affects all incoming packet types and is always used if configured. If configured next-hop is not present in the routing table, an ARP request is sent from the switch.

In a route-map statement, the **set ip next-hop** and **set ip default next-hop** commands are mutually exclusive. However, the **set ip default next-hop** command can be configured in a separate route map statement.

You can specify a maximum of 16 next-hop IP addresses.

Format	set ip next-hop <i>ip-address</i> [... <i>ip-address</i>]

Mode	Route Map Configuration

Parameter	Description
ip-address	The IP address of the next hop to which packets are output. It must be the address of an adjacent router.

no set ip next-hop

Use this command to remove a set command from a route map.

Format	no set ip next-hop <i>ip-address</i> [... <i>ip-address</i>]

Mode	Route Map Configuration

set ip default next-hop

M4250**M4350**

Use this command to set a list of default next-hop IP addresses. If more than one IP address is specified, the first next hop specified that appears to be adjacent to the switch is used. The optional specified IP addresses are tried in turn.

A packet is routed to the next hop specified by this command only if there is no active route for the packet's destination address in the routing table. A default route in the routing table is not considered an active route for an unknown destination address for policy-based routing (PBR).

In a route-map statement, the **set ip next-hop** and **set ip default next-hop** commands are mutually exclusive. However, the **set ip default next-hop** command can be configured in a separate route-map statement.

You can specify a maximum of 16 next-hop IP addresses.

Format	<code>set ip default next-hop ip-address [...ip-address]</code>
Mode	Route Map Configuration
Parameter	Description
ip-address	The IP address of the next hop to which packets are output. It must be the address of an adjacent router.

no set ip default next-hop

Use this command to remove a set command from a route map.

Format	<code>no set ip default next-hop ip-address [...ip-address]</code>
Mode	Route Map Configuration

set ip precedence

M4250**M4350**

Use this command to set the three IP precedence bits in the IP packet header. With three bits, you have eight possible values for the IP precedence; *value* can be a number from 0 through 7. This command is used when implementing QoS and can be used by other QoS services, such as weighted fair queuing (WFQ) and weighted random early detection (WRED).

Default	No precedence set
Format	<code>set ip precedence value</code>
Mode	Route Map Configuration

Parameter	Description
0	Sets the routine precedence
1	Sets the priority precedence
2	Sets the immediate precedence
3	Sets the Flash precedence
4	Sets the Flash override precedence
5	Sets the critical precedence
6	Sets the internetwork control precedence
7	Sets the network control precedence

`no set ip precedence`

Use this command to reset the three IP precedence bits in the IP packet header to the default.

Format	<code>no set ip precedence</code>
Mode	Route Map Configuration

`show ip policy`

M4250

M4350

This command lists the route map associated with each interface.

Format	<code>show ip policy</code>
Mode	Privileged Exec

Term	Definition
Interface	The interface.
Route-map	The route map

show route-map

M4250

M4350

To display a route map, use the **show route-map** command in Privileged EXEC mode.

Format	show route-map [<i>map-name</i>]
Mode	Privileged EXEC
Parameter	Description
map-name	(Optional) Name of a specific route map.

Command example:

```
(NETGEAR Switch) # show route-map test
route-map test, permit, sequence 10
  Match clauses:
    ip address prefix-lists: orange
  Set clauses:
    set metric 50
```

Router Discovery Protocol Commands

This section describes the commands you use to view and configure Router Discovery Protocol (RDP) settings on the switch. The Router Discovery Protocol enables a host to discover the IP address of routers on the subnet.

ip irdp

M4250

M4350

This command enables router discovery on an interface or range of interfaces.

Default	disabled
Format	ip irdp
Mode	Interface Config

no ip irdp

This command disables router discovery on an interface.

Format	no ip irdp

Mode	Interface Config

ip irdp address

M4250

M4350

This command configures the address that the interface uses to send the router discovery advertisements. The valid values for *ipaddr* are 224.0.0.1, which is the all-hosts IP multicast address, and 255.255.255.255, which is the limited broadcast address.

Default	224.0.0.1

Format	ip irdp address <i>ipaddr</i>

Mode	Interface Config

no ip irdp address

This command configures the default address that is used for router advertisements on the interface.

Format	no ip irdp address

Mode	Interface Config

ip irdp holdtime

M4250

M4350

This command configures the value of the hold time field of the router advertisement sent from this interface. The *seconds* argument hold time value is in the range from 4 to 9000 seconds.

Default	3 * maxinterval

Format	ip irdp holdtime <i>seconds</i>

Mode	Interface Config

no ip irdp holdtime

This command resets the default value of the hold time field of the router advertisement sent from this interface.

Format	no ip irdp holdtime

Mode	Interface Config

ip irdp maxadvertinterval

M4250

M4350

This command configures the maximum time allowed between sending router advertisements from the interface. The range for the *seconds* argument is 4 to 1800 seconds.

Default	600

Format	ip irdp maxadvertinterval <i>seconds</i>

Mode	Interface Config

no ip irdp maxadvertinterval

This command resets the default maximum time.

Format	no ip irdp maxadvertinterval

Mode	Interface Config

ip irdp minadvertinterval

M4250

M4350

This command configures the minimum time allowed between sending router advertisements from the interface. The range for *seconds* argument is 3–1800 seconds.

Default	0.75 * maxadvertinterval

Format	ip irdp minadvertinterval <i>seconds</i>

Mode	Interface Config

no ip irdp minadvertinterval

This command resets the default minimum time to the default.

Format	no ip irdp minadvertinterval

Mode	Interface Config

ip irdp multicast

M4250

M4350

This command configures the destination IP address for router advertisements as 224.0.0.1, which is the default address. The *no* form of the command configures the IP address as 255.255.255.255 to instead send router advertisements to the limited broadcast address.

Format	ip irdp multicast

Mode	Interface Config

no ip irdp multicast

By default, router advertisements are sent to 224.0.0.1. To instead send router advertisements to the limited broadcast address, 255.255.255.255, use the *no* form of this command.

Format	no ip irdp multicast

Mode	Interface Config

ip irdp preference

M4250

M4350

This command configures the preferability of the address as a default router address, relative to other router addresses on the same subnet. The preference *number* can be a number from -2147483648 to 2147483647.

Default	0

Format	ip irdp preference <i>number</i>

Mode	Interface Config

no ip irdp preference

This command configures the default preferability of the address as a default router address, relative to other router addresses on the same subnet.

Format	no ip irdp preference
Mode	Interface Config

show ip irdp

M4250

M4350

This command displays the router discovery information for all interfaces, a specified interface, or specified VLAN. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* argument are used to specify the VLAN ID of the routing VLAN. The *vlan-id* argument can be a number from 1–4093.

Format	show ip irdp {unit/slot/port vlan vlan-id all}
Modes	Privileged EXEC User EXEC

Term	Definition
Interface	The interface that corresponds to a physical routing interface or VLAN routing interface.
vlan	Use this keyword to specify the VLAN ID of the routing VLAN.
Ad Mode	The advertise mode, which indicates whether router discovery is enabled or disabled on this interface.
Dest Address	The destination IP address for router advertisements.
Max Int	The maximum advertise interval, which is the maximum time, in seconds, allowed between sending router advertisements from the interface.
Min Int	The minimum advertise interval, which is the minimum time, in seconds, allowed between sending router advertisements from the interface.
Hold Time	The amount of time, in seconds, that a system should keep the router advertisement before discarding it.
Preference	The preference of the address as a default router address, relative to other router addresses on the same subnet.

Virtual LAN Routing Commands

This section describes the commands you use to view and configure VLAN routing and to view VLAN routing status information.

vlan routing

M4250

M4350

This command enables routing on a VLAN. The *vlanid* value has a range from 1 to 4093. The *interface-id* value has a range from 1 to 128. Typically, you do not supply the interface ID argument, and the system automatically selects the interface ID. However, if you specify an interface ID, the interface ID becomes the port number in the *slot/port* (M4250 series switch) or *unit/slot/port* (M4350 series switch) for the VLAN routing interface.

If you select an interface ID that is already in use, the CLI displays an error message and does not create the VLAN interface. For products that use text-based configuration, including the interface ID in the **vlan routing** command for the text configuration ensures that the *slot/port* (M4250 series switch) or the *unit/slot/port* (M4350 series switch) for the VLAN interface stays the same across a restart. Keeping the *slot/port* (M4250 series switch) or the *unit/slot/port* (M4350 series switch) the same ensures that the correct interface configuration is applied to each interface when the system restarts.

Format	<code>vlan routing vlanid [interface-id]</code>
Mode	VLAN Config (also referred to as VLAN Database)

no vlan routing

This command deletes routing on a VLAN.

Format	<code>no vlan routing vlanid</code>
Mode	VLAN Config (also referred to as VLAN Database)

Command example:

The following example specifies a VLAN ID value. The interface ID argument is not used.

```
(NETGEAR Switch) (Vlan) #vlan 14
(NETGEAR Switch) (Vlan) #vlan routing 14 ?
<cr>                               Press enter to execute the command.
<1-24>                             Enter interface ID
```

Typically, you press **Enter** without supplying the Interface ID value; the system automatically selects the interface ID.

Command example:

The following example specifies interface ID 51 for VLAN 14 interface. The interface ID becomes the port number in the *slot/port* (M4250 series switch) or *unit/slot/port* (M4350 series switch) for the VLAN routing interface. for the VLAN routing interface.

In this example, *unit/slot/port* is 4/51 for the VLAN 14 interface.

```
(NETGEAR Switch) (Vlan) #vlan 14 51
```

```
(NETGEAR Switch) (Vlan) #
```

```
(NETGEAR Switch) #show ip vlan
```

```
MAC Address used by Routing VLANs: 00:11:88:59:47:36
```

VLAN ID	Logical		
	Interface	IP Address	Subnet Mask
10	4/1	172.16.10.1	255.255.255.0
11	4/50	172.16.11.1	255.255.255.0
12	4/3	172.16.12.1	255.255.255.0
13	4/4	172.16.13.1	255.255.255.0
14	4/51	0.0.0.0	0.0.0.0 <--u/s/p is 4/51 for VLAN 14 interface

Command example:

The following example selects an interface ID that is already in use. In this case, the CLI displays an error message and does not create the VLAN interface.

```
(NETGEAR Switch) #show ip vlan
```

```
MAC Address used by Routing VLANs: 00:11:88:59:47:36
```

VLAN ID	Logical		
	Interface	IP Address	Subnet Mask
10	4/1	172.16.10.1	255.255.255.0
11	4/50	172.16.11.1	255.255.255.0
12	4/3	172.16.12.1	255.255.255.0
13	4/4	172.16.13.1	255.255.255.0
14	4/51	0.0.0.0	0.0.0.0

```
(NETGEAR Switch) #config
```

```
(NETGEAR Switch) (Config) #exit
```

```
(NETGEAR Switch) #vlan database
```

```
(NETGEAR Switch) (Vlan) #vlan 15
```

```
(NETGEAR Switch) (Vlan) #vlan routing 15 1
```

```
Interface ID 1 is already assigned to another interface
```

Command example:

The **show running-config** command lists the interface ID for each routing VLAN:

```
(NETGEAR Switch) #show running-config
!!Current Configuration:
!
!System Description "NETGEAR M4350-12X12F 12x10G Copper 12x10G SFP+ Managed Switch,
14.0.0.15, 1.0.0.4"
!System Software Version "14.0.0.15"
!System Up Time          "0 days 0 hrs 23 mins 7 secs"
!Additional Packages      QOS,Multicast,IPv6,IPv6 Management,Routing
!Current SNTP Synchronized Time: SNTP Client Mode Is Disabled
!
vlan database
exit

configure
no logging console
aaa authentication enable "enableNetList" none
line console
serial timeout 0
exit

line telnet
exit

line ssh
exit

!
router rip
exit
exit
```

interface vlan

M4250

M4350

Use this command to enter Interface configuration mode for the specified VLAN. The vlan-id range is 1 to 4093.

Format	interface vlan <i>vlan-id</i>
Mode	Global Config

autostate

M4250

M4350

The autostate feature is enabled on all VLAN routing interfaces by default. In this mode, when all ports in the VLAN are down, the IP interface for that VLAN is also down.

Default	Enabled
Format	autostate
Mode	Interface Config

no autostate

This command configures the VLAN routing interface to remain up, even if there are no ports that are members of the VLAN. The switch responds to the pings on that IP address.

Format	no autostate
Mode	Interface Config

show ip vlan

M4250

M4350

This command displays the VLAN routing information for all VLANs with routing enabled.

Format	show ip vlan
Modes	Privileged EXEC User EXEC

Term	Definition
MAC Address used by Routing VLANs	The MAC Address associated with the internal bridge-router interface (IBRI). The same MAC Address is used by all VLAN routing interfaces. It will be displayed above the per-VLAN information.
VLAN ID	The identifier of the VLAN.
Logical Interface	The logical <i>unit/slot/port</i> associated with the VLAN routing interface.
IP Address	The IP address associated with this VLAN.
Subnet Mask	The subnet mask that is associated with this VLAN.

Virtual Router Redundancy Protocol Commands

Note: Virtual Router Redundancy Protocol (VRRP) commands are supported on the M4350 series switches only. The M4250 series switches do not support VRRP.

This section describes the commands you use to view and configure VRRP and to view VRRP status information. VRRP helps provide failover and load balancing when you configure two devices as a VRRP pair.

ip vrrp (Global Config)

M4350

Use this command in Global Config mode to enable the administrative mode of VRRP on the switch.

Default	none
Format	ip vrrp
Mode	Global Config

no ip vrrp

Use this command in Global Config mode to disable the default administrative mode of VRRP on the switch.

Format	no ip vrrp
Mode	Global Config

ip vrrp (Interface Config)

M4350

Use this command in Interface Config mode to create a virtual router associated with the interface or range of interfaces. The parameter *vrid* is the virtual router ID, which has an integer value range from 1 to 255.

Format	ip vrrp vrid
Mode	Interface Config

no ip vrrp

Use this command in Interface Config mode to delete the virtual router associated with the interface. The virtual router ID, *vrid*, is an integer value that ranges from 1 to 255.

Format	no ip vrrp <i>vrid</i>
Mode	Interface Config

ip vrrp mode

M4350

This command enables the virtual router configured on the specified interface. Enabling the status field starts a virtual router. The parameter *vrid* is the virtual router ID which has an integer value ranging from 1 to 255.

Default	disabled
Format	ip vrrp <i>vrid</i> mode
Mode	Interface Config

no ip vrrp mode

This command disables the virtual router configured on the specified interface. Disabling the status field stops a virtual router. The parameter *vrid* is the virtual router ID which has an integer value ranging from 1 to 255.

Format	no ip vrrp <i>vrid</i> mode
Mode	Interface Config

ip vrrp ip

M4350

This command sets the virtual router IP address value for an interface or range of interfaces. The value for *ipaddr* is the IP address which is to be configured on that interface for VRRP. The parameter *vrid* is the virtual router ID which has an integer value range from 1 to 255.

You can use the optional **secondary** keyword to designate the IP address as a secondary IP address.

Default	none
Format	ip vrrp <i>vrid</i> ip <i>ipaddr</i> [secondary]
Mode	Interface Config

no ip vrrp ip

Use this command in Interface Config mode to delete a secondary IP address value from the interface. To delete the primary IP address, you must delete the virtual router on the interface.

The value for *ipaddr* is the IP address which is to be configured on that interface for VRRP. The parameter *vrid* is the virtual router ID which has an integer value range from 1 to 255.

Format	no ip vrrp vrid ipaddress secondary

Mode	Interface Config

ip vrrp accept-mode

M4350

Use this command to allow the VRRP primary router to accept ping packets sent to one of the virtual router's IP addresses. The parameter *vrid* is the virtual router ID which has an integer value range from 1 to 255.

Note: VRRP accept-mode allows only ICMP Echo Request packets. No other type of packet is allowed to be delivered to a VRRP address.

Default	disabled

Format	ip vrrp vrid accept-mode

Mode	Interface Config

no ip vrrp accept-mode

Use this command to prevent the VRRP primary router from accepting ping packets sent to one of the virtual router's IP addresses. The parameter *vrid* is the virtual router ID which has an integer value range from 1 to 255.

Format	no ip vrrp vrid accept-mode

Mode	Interface Config

ip vrrp authentication

M4350

This command sets the authorization details value for the virtual router configured on a specified interface or range of interfaces. The parameter **none** or **simple** specifies the authorization type for virtual router configured on the specified interface. The parameter *key* is optional and is only required when authorization type is a simple text password. The parameter *vrid* is the virtual router ID which has an integer value ranges from 1 to 255.

Default	no authorization

Format	ip vrrp vrid authentication {none simple key}

Mode	Interface Config

no ip vrrp authentication

This command sets the default authorization details value for the virtual router configured on a specified interface or range of interfaces. The parameter *vrid* is the virtual router ID which has an integer value ranges from 1 to 255.

Format	no ip vrrp vrid authentication

Mode	Interface Config

ip vrrp preempt

M4350

This command sets the preemption mode value for the virtual router configured on a specified interface or range of interfaces. The parameter *vrid* is the virtual router ID which has an integer value ranges from 1 to 255.

Default	enabled

Format	ip vrrp vrid preempt

Mode	Interface Config

no ip vrrp preempt

This command sets the default preemption mode value for the virtual router configured on a specified interface or range of interfaces. The parameter *vrid* is the virtual router ID which has an integer value ranges from 1 to 255.

Format	no ip vrrp vrid preempt

Mode	Interface Config

ip vrrp priority

M4350

This command sets the priority of a router within a VRRP group. It can be used to configure an interface or a range of interfaces. Higher values equal higher priority. The range is from 1 to 254. The parameter *vrid* is the virtual router ID which has an integer value ranges from 1 to 255.

The router with the highest priority is elected the primary router. If a router is configured with the address used as the address of the virtual router, the router is called the address owner. The priority of the address owner is always 255 so that the address owner is always the primary router. If the primary router has a priority less than 255 (it is not the address owner) and you configure the priority of another router in the group higher than the primary router's priority, the router will take over as the primary router only if preempt mode is enabled.

Default	100 unless the router is the address owner, in which case its priority is automatically set to 255.
Format	<code>ip vrrp vrid priority priority</code>
Mode	Interface Config

no ip vrrp priority

This command sets the default priority value for the virtual router configured on a specified interface or range of interfaces. The parameter *vrid* is the virtual router ID which has an integer value ranges from 1 to 255.

Format	<code>no ip vrrp vrid priority</code>
Mode	Interface Config

ip vrrp timers advertise

M4350

This command sets the frequency, from 1–255 seconds, that an interface or range of interfaces on the specified virtual router sends a virtual router advertisement. The parameter *vrid* is the virtual router ID which has an integer value ranges from 1 to 255.

Default	1
Format	<code>ip vrrp vrid timers advertise seconds</code>
Mode	Interface Config

no ip vrrp timers advertise

This command sets the default virtual router advertisement value for an interface or range of interfaces. The parameter *vrid* is the virtual router ID which has an integer value ranges from 1 to 255.

Format	<code>no ip vrrp vrid timers advertise</code>
Mode	Interface Config

ip vrrp track interface

M4350

Use this command to alter the priority of the VRRP router based on the availability of its interfaces. This command is useful for tracking interfaces that are not configured for VRRP. The parameter *vrid* is the virtual router ID which has an integer value ranges from 1 to 255. Only IP interfaces are tracked. A tracked interface is up if the IP on that interface is up. Otherwise, the tracked interface is down. You can use this command to configure a single interface or range of interfaces. The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* can be a number from 1–4093.

When the tracked interface is down or the interface is removed from the router, the priority of the VRRP router is decremented by the value specified in the *priority* argument. When the interface is up for the IP protocol, the priority is incremented by the *priority* value.

A VRRP-configured interface can track more than one interface. When a tracked interface goes down, the priority of the router is decreased by 10 (the default priority decrement) for each interface that is down. The default priority decrement is changed using the *priority* argument. The default priority of the virtual router is 100, and the default decrement priority is 10. By default, no interfaces are tracked. If you specify just the interface to be tracked, without the optional priority, the default priority is set. The default priority decrement is 10.

Default	priority: 10
Format	<code>ip vrrp vrid track interface {unit/slot/port vlan vlan-id} [decrement priority]</code>
Mode	Interface Config

no ip vrrp track interface

Use this command to remove the interface or range of interfaces from the tracked list or to restore the priority decrement to its default. The parameter *vrid* is the virtual router ID which has an integer value ranges from 1 to 255.

Format	<code>no ip vrrp vrid track interface {unit/slot/port vlan vlan-id} [decrement]</code>
Mode	Interface Config

ip vrrp track ip route

M4350

Use this command to track the route reachability on an interface or range of interfaces. The parameter *vrid* is the virtual router ID which has an integer value ranges from 1 to 255. When the tracked route is deleted, the priority of the VRRP router will be decremented by the value specified in the *priority* argument. When the tracked route is added, the priority will be incremented by the same.

A VRRP configured interface can track more than one route. When a tracked route goes down, the priority of the router is decreased by 10 (the default priority decrement) for each route that is down. By default no routes are tracked. If you specify just the route to be tracked, without the optional priority, the default priority is set. The default priority decrement is 10. The default priority decrement is changed using the *priority* argument.

Default	priority: 10
Format	<code>ip vrrp vrid track ip route ip-address/prefix-length [decrement priority]</code>
Mode	Interface Config

`no ip vrrp track ip route`

Use this command to remove the route from the tracked list or to restore the priority decrement to its default. When removing a tracked IP route from the tracked list, the priority should be incremented by the decrement value if the route is not reachable. The parameter *vrid* is the virtual router ID which has an integer value ranges from 1 to 255.

Format	<code>no ip vrrp vrid track interface unit/slot/port [decrement]</code>
Mode	Interface Config

`show ip vrrp`

M4350

This command displays whether VRRP functionality is enabled or disabled on the switch. It also displays some global parameters which are required for monitoring.

Format	<code>show ip vrrp</code>
Modes	Privileged EXEC User EXEC

Term	Definition
VRRP Admin Mode	The administrative mode for VRRP functionality on the switch.
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 Unknown or unsupported version number.
Router VRID Errors	The total number of VRRP packets received with invalid VRID for this virtual router.

show ip vrrp interface

M4350

This command displays all configuration information and VRRP router statistics of a virtual router configured on a specific interface. The parameter *vrid* is the virtual router ID which has an integer value ranges from 1 to 255.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* can be a number from 1–4093.

Format	<code>show ip vrrp interface {unit/slot/port vlan vlan-id} vrid</code>
Modes	Privileged EXEC User EXEC

Term	Definition
IP Address	The configured IP address for the virtual router.
VMAC address	The VMAC address of the specified router.
Authentication type	The authentication type for the specific virtual router.
Priority	The priority value for the specific virtual router, taking into account any priority decrements for tracked interfaces or routes.
Configured Priority	The priority configured through the <code>ip vrrp vrid priority priority</code> command.
Advertisement interval	The advertisement interval in seconds for the specific virtual router.
Pre-Empt Mode	The preemption mode configured on the specified virtual router.
Administrative Mode	The status (Enable or Disable) of the specific router.
Accept Mode	When enabled, the VRRP primary router can accept ping packets sent to one of the virtual router's IP addresses.
State	The state of the virtual router.

Command example:

```
show ip vrrp interface <u/s/p> vrid
```

```

Primary IP Address..... 1.1.1.5
VMAC Address..... 00:00:5e:00:01:01
Authentication Type..... None
Priority..... 80
    Configured priority..... 100
Advertisement Interval (secs)..... 1
Pre-empt Mode..... Enable
Administrative Mode..... Enable

```

```

Accept Mode..... Enable
State..... Initialized
Track Interface      State      DecrementPriority
-----
<1/0/1>              down        10

TrackRoute  (pfx/len)  State      DecrementPriority
-----
10.10.10.1/255.255.255.0  down        10

```

show ip vrrp interface brief

M4350

This command displays information about each virtual router configured on the switch. It displays information about each virtual router.

Format	show ip vrrp interface brief
Modes	Privileged EXEC User EXEC
Term	Definition
Interface	The interface number.
VRID	The router ID of the virtual router.
IP Address	The virtual router IP address.
Mode	Indicates whether the virtual router is enabled or disabled.
State	The state (primary/backup) of the virtual router.

show ip vrrp interface stats

M4350

This command displays the statistical information about each virtual router configured on the switch. The parameter *vrid* is the virtual router ID which has an integer value ranges from 1 to 255.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* can be a number from 1–4093.

Format	show ip vrrp interface stats {unit/slot/port vlan vlan-id} vrid
Modes	Privileged EXEC User EXEC

Term	Definition
Uptime	The time that the virtual router has been up, in days, hours, minutes and seconds.
Protocol	The protocol configured on the interface.
State Transitioned to Master	The total number of times the virtual router state has changed to primary router.
Advertisement Received	The total number of VRRP advertisements received by this virtual router.
Advertisement Interval Errors	The total number of VRRP advertisements received for which advertisement interval is different than the configured value for this virtual router.
Authentication Failure	The total number of VRRP packets received that don't pass the authentication check.
IP TTL errors	The total number of VRRP packets received by the virtual router with IP TTL (time to live) not equal to 255.
Zero Priority Packets Received	The total number of VRRP packets received by 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 total number of VRRP packets received by the virtual router with invalid 'type' field.
Address List Errors	The total number of VRRP packets received for which address list does not match the locally configured list for the virtual router.
Invalid Authentication Type	The total number of VRRP packets received with unknown authentication type.
Authentication Type Mismatch	The total number of VRRP advertisements received for which the authentication type is not equal to the locally configured type for this virtual router.
Packet Length Errors	The total number of VRRP packets received with packet length less than length of VRRP header.

show vrrp

M4350

This command displays information for all active VRRPv3 groups (if you enter the command without any optional parameters), all active VRRPv3 groups that are configured in an IPv4 or IPv6 address family (if you use the **ipv4** or **ipv6** keyword), or the active VRRPv3 groups configured in an IPv4 or IPv6 address family for a specified interface or VLAN.

This command displays the statistical information about each virtual router configured on the switch. The parameter *vrid* is the virtual router ID, which has A value ranges from 1 to 255.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* can be a number from 1–4093.

Format	show vrrp [{ipv4 ipv6}] [{unit/slot/port vlan vlan-id} vrid]

Modes	Privileged EXEC
	User EXEC

Command example:

This example shows command output when no parameters are specified.

```
(NETGEAR Switch)#show vrrp
```

```
Admin Mode..... Enable
```

```
1/0/2 - VRID 1 - Address-Family IPv4
```

```
Virtual IP address..... 1.1.1.9
Secondary IP Address(es)..... 1.1.1.4
..... 1.1.1.5
..... 1.1.1.6
Virtual MAC Address..... 00:00:5e:00:01:01
Priority..... 0
Configured Priority..... 111
Advertisement Interval..... 120 centisec
Pre-empt Mode..... Enable
Accept Mode..... Enable
Administrative Mode..... Enable
State..... Initialized
Master Router IP / Priority..... 1.1.1.3 (local) / 100
Master Advertisement interval..... 120 centisec
Master Down interval..... 360 centisec
```

```
Track Interface State DecrementPriority BFD-Neighbor
```

```
-----
1/0/9          Down  222      23.10.8.6
```

```
Track Route(pfx/len)  Reachable  DecrementPriority
```

```
-----
14.14.14.0/24         True      14
```

```
1/0/3 - VRID 2 - Address-Family IPv4
```

```
Virtual IP address..... 3.3.2.9
```

Fully Managed Switches M4250 and M4350 Series

```

Secondary IP Address(es)..... 3.3.2.4
..... 3.3.2.5
..... 3.3.2.6
Virtual MAC Address..... 00:00:5e:00:01:06
Priority..... 0
Configured Priority..... 130
Advertisement Interval..... 120 centisec
Pre-empt Mode..... Enable
Accept Mode..... Enable
Administrative Mode..... Enable
State..... Initialized
Master Router IP / Priority..... 1.1.1.3 (local) / 100
Master Advertisement interval..... 120 centisec
Master Down interval..... 360 centisec

```

```

Track Interface State DecrementPriority   BFD-Neighbor
-----
1/0/7          Down  125          55.16.27.8

```

```

Track Route (pfx/len)   Reachable  DecrementPriority
-----
14.14.14.0/24          True      30

```

1/0/12 - VRID 3 - Address-Family IPv6

```

Virtual IP address..... 4001::2
Secondary IP Address(es)..... 4001::5
..... 4001::6
..... 4001::7
Virtual MAC Address..... 00:00:5e:00:01:06
Priority..... 0
Configured Priority..... 130
Advertisement Interval..... 120 centisec
Pre-empt Mode..... Enable
Accept Mode..... Enable
Administrative Mode..... Enable
State..... Initialized
Master Router IP / Priority..... 4001::3 (local) / 100
Master Advertisement interval..... 120 centisec
Master Down interval..... 360 centisec

```

```

Track Interface State DecrementPriority   BFD-Neighbor
-----
1/0/2          Down  250          5001::3

```


Track Route(pfx/len)	Reachable	DecrementPriority
4004::3/32	True	20

Command example:

This example shows command output when the IPv4 parameter is specified.

```
(NETGEAR Switch)#show vrrp ipv4
```

```
Admin Mode..... Enable
```

```
1/0/2 - VRID 1 - Address-Family IPv4
```

```
Virtual IP address..... 1.1.1.9
Secondary IP Address(es)..... 1.1.1.4
..... 1.1.1.5
..... 1.1.1.6
Virtual MAC Address..... 00:00:5e:00:01:01
Priority..... 0
Configured Priority..... 111
Advertisement Interval..... 120 centisec
Pre-empt Mode..... Enable
Accept Mode..... Enable
Administrative Mode..... Enable
State..... Initialized
Master Router IP / Priority..... 1.1.1.3 (local) / 100
Master Advertisement interval..... 120 centisec
Master Down interval..... 360 centisec
```

```
Track Interface State DecrementPriority
```

```
-----
1/0/9          Down  222
```

Track Route(pfx/len)	Reachable	DecrementPriority
14.14.14.0/24	True	14

```
1/0/3 - VRID 2 - Address-Family IPv4
```

```
Virtual IP address..... 3.3.2.9
Secondary IP Address(es)..... 3.3.2.4
..... 3.3.2.5
..... 3.3.2.6
Virtual MAC Address..... 00:00:5e:00:01:06
Priority..... 0
```

```

Configured Priority..... 130
Advertisement Interval..... 120 centisec
Pre-empt Mode..... Enable
Accept Mode..... Enable
Administrative Mode..... Enable
State..... Initialized
Master Router IP / Priority..... 1.1.1.3 (local) / 100
Master Advertisement interval..... 120 centisecsec
Master Down interval..... 360

```

Track Interface State DecrementPriority

```

-----
1/0/7          Down  125

```

Track Route (pfx/len) Reachable DecrementPriority

```

-----
14.14.14.0/24   True    30

```

Command example:

This example shows command output when the IPv6 parameter is specified.

```
(NETGEAR Switch)#show vrrp ipv6
```

```
Admin Mode..... Enable
```

```
1/0/2 - VRID 1 - Address-Family IPv6
```

```

Virtual IP address..... 1001::8
Secondary IP Address(es)..... 1001::5
..... 1001::6
..... 1001::7
Virtual MAC Address..... 00:00:5e:00:01:01
Priority..... 0
Configured Priority..... 100
Advertisement Interval..... 100 centisec
Pre-empt Mode..... Enable
Accept Mode..... Enable
Administrative Mode..... Enable
State..... Initialized
Master Router IP / Priority..... 1001::1 (local) / 100
Master Advertisement interval..... 100 centisec
Master Down interval..... 300 centisec

```

Track Interface State DecrementPriority

```

-----
1/0/9          Down  222

```

Fully Managed Switches M4250 and M4350 Series

Track Route(pfx/len)	Reachable	DecrementPriority
-----	-----	-----
2001::2/32	True	14

1/0/12 - VRID 3 - Address-Family IPv6

```

Virtual IP address..... 4001::2
Secondary IP Address(es)..... 4001::5
..... 4001::6
..... 4001::7
Virtual MAC Address..... 00:00:5e:00:01:06
Priority..... 130
Configured Priority..... 130
Advertisement Interval..... 120 centisec
Pre-empt Mode..... Enable
Accept Mode..... Enable
Administrative Mode..... Enable
State..... Master
Master Router IP / Priority..... 4001::3 (local) / 130
Master Advertisement interval..... 120 centisec
Master Down interval..... 360 centisec

```

Track Interface State	DecrementPriority
-----	-----
1/0/24 Down	320

Track Route(pfx/len)	Reachable	DecrementPriority
-----	-----	-----
7003::4/32	True	50

Command example:

This example shows command output when the IPv4 parameter is specified with an interface.

```
(NETGEAR Switch)#show vrrp ipv4 1/0/3 1
```

```

Virtual IP address..... 1.1.1.9
Secondary IP Address(es)..... 1.1.1.4
..... 1.1.1.5
..... 1.1.1.6
Virtual MAC Address..... 00:00:5e:00:01:01
Priority..... 0
Configured Priority..... 111
Advertisement Interval..... 222 centisec

```

Fully Managed Switches M4250 and M4350 Series

```
Pre-empt Mode..... Enable
Accept Mode..... Enable
Administrative Mode..... Enable
State..... Initialized
Master Router IP / Priority..... 1.1.1.3 (local) / 100
Master Advertisement interval..... 1000 centisec
Master Down interval..... 3000 centisec
```

```
Track Interface State Decrement-Priority
```

```
-----
0/9          Down  222
```

```
Track Route (pfx/len)  Reachable  Decrement-Priority
-----
14.14.14.0/24         True        14
```

show vrrp brief

M4350

This command displays brief information for all active VRRPv3 groups.

Format	show vrrp brief
Modes	Privileged EXEC User EXEC

Term	Definition
Interface	The interface on which VRRP is configured.
VR	The ID of the virtual router.
A-F	The IP address family type (IPv4 or Ipv6) to which the virtual router belongs.
Pri	The priority range of the virtual router.
AdvIntvl	The advertisement interval configured for the virtual router.
Pre	The preemption state of the virtual router.
Acc	The accept mode of the virtual router.
State	The VRRP group state, which can be one of the following: Init, Backup, or Master.
VR IP address	The virtual IP address for the VRRP group.

Command example:

```
(NETGEAR Switch)#show vrrp brief
```

Interface	VRID	A-F	Pri	AdvIntvl	Pre	Acc	State	VR IP Address
1/0/1	1	IPv4	100	200s	Y	Y	Init	192.0.1.10
1/0/3	2	IPv4	200	200s	Y	Y	Init	124.0.3.17
1/0/1	7	IPv6	100	200s	Y	Y	Backup	5002::1
1/0/5	2	IPV6	20	200s	Y	Y	Master	2001::2

show vrrp statistics**M4350**

This command displays statistical information for a VRRPv3 group. If you do not include optional arguments, the command displays the global statistics.

If the specify optional arguments, the statistics are displayed for the virtual router that corresponds to the a combination of an IP address family, interface, and virtual router ID (*vrid*), which is a value ranges from 1 to 255.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* can be a number from 1–4093.

Format	show vrrp statistics [{ipv4 ipv6} {unit/slot/port vlan vlan-id} {vrid}]
Modes	Privileged EXEC User EXEC

Command example:

This example shows command output when no parameters are specified.

```
(NETGEAR Switch)#show vrrp statistics
```

```
Router Checksum Errors..... 2
Router Version Errors..... 3
Router VRID Errors..... 4
Global Statistics Discontinuity Time..... 0 days 0 hrs 0 mins 0 secs
```

Command example:

This example shows command output when the IPv6 parameter is specified, along with an tinterface and a VRID.

```
(NETGEAR Switch)#show vrrp statistics ipv6 1/0/1 2
```

```
Master Transitions..... 2
New Master Reason..... Priority
```

```

Advertisements Received..... 64
Advertisements Sent..... 12
Advertisement Interval Errors..... 0
IP TTL Errors..... 1
Last Protocol Error Reason..... Version Error
Zero Priority Packets Received..... 0
Zero Priority Packets Sent..... 1
Invalid Type Packets Received..... 0
Address List Errors..... 2
Packet Length Errors..... 4
Row Discontinuity Time..... 0 days 0 hrs 0 mins 0 secs
Refresh Rate (in milliseconds)..... 0

```

clear ip vrrp interface stats

M4350

This command clears VRRP statistical information from an interface or a VLAN. The virtual router ID, *vrid*, is an integer value that ranges from 1 to 255.

Format	clear ip vrrp interface stats {unit/slot/port vrid vlan vlan-id vrid}
Modes	Interface Config

Virtual Router Redundancy Protocol version 3 Commands

Note: Virtual Router Redundancy Protocol version 3 (VRRPv3) commands are supported on the M4350 series switches only. The M4250 series switches do not support VRRPv3.

VRRPv3 provides address redundancy for both IPv4 and IPv6 router addresses. VRRPv3 support is similar to VRRP support. The following table provides a summary of the differences.

VRRP2	VRRPv3
Supports redundancy for IPv4 addresses.	Supports redundancy for IPv4 and IPv6 addresses.
Supports authentication.	Does not support authentication.
No link-local address support for IPv4 addresses.	For IPv6 addresses, VRRP IP contains the link-local IPv6 address too.

VRRP2	VRRPv3
The interval time used for sending VRRP Advertisement packets is in seconds.	The interval time used for sending VRRP Advertisement packets is in centiseconds.
The VRRP MAC address format is 00-00-5E-00-01-{VRID}	The VRRP MAC address format for IPv6 VRRP is 00-00-5E-00-02-{VRID}
SNMP MIB RFC according to 2787. The counters are 32-bit counters.	SNMP MIB RFC as per RFC 6527. The counters are 64-bit counters.

To enable VRRP on the switch, use the **ip vrrp** command. This command enables VRRP (v2 or v3, depending on which version is the configured version) and makes it operational.

fhrp version vrrp vc3

M4350

To enable Virtual Router Redundancy Protocol version 3 (VRRPv3) configuration on a device, use the **fhrp version vrrp v3** command in global configuration mode.

When VRRPv3 is in use, VRRP version 2 (VRRPv2) is unavailable. If you enter the **no fhrp version vrrp v3** command, VRRPv3 is disabled and VRRPv2 is enabled. Also, operational data is reset, and the VRRPv2 configuration is applied. The same guidelines apply when VRRPv2 is in use and you enter the **no ip vrrp** command.

Default	Disabled
Format	fhrp version vrrp v3
Mode	Global Config

no fhrp version vrrp vc3

This command disables VRRPv3 on the switch and enabled VRRPv2 on the switch.

Format	no fhrp version vrrp v3
Mode	Global Config

vrrp address-family

M4350

If VRRPv3 is configured, this command creates a VRRPv3 group on an interface and lets the CLI enter VRRPv3 configuration mode.

Format	vrrp group-id address-family {ipv4 ipv6}
Mode	Interface Config

Parameter	Definition
<i>group-id</i>	The virtual router group number, which is the range from 1 to 255.
ipv4	An IPv4 address family for this VRRP group.
ipv6	An IPv6 address family for this VRRP group.

Command example:

```
(NETGEAR Switch) (Config) #interface 1/0/7
(NETGEAR Switch) (Interface 1/0/7) #vrrp 22 address-family ipv4
(NETGEAR Switch) (config-if-vrrp)
```

```
no vrrp address-family
```

This command removes a VRRPv3 group from an interface.

Before you can use this command, you must disable virtual router using the **shutdown** command in the appropriate VRRP Config mode.

Format	<code>no vrrp group-id address-family {ipv4 ipv6}</code>
Mode	Interface Config

preempt (VRRPv3 Config mode)

M4350

This command configures the switch to take over as the primary virtual router for a VRRP group if the switch has a higher priority than the current primary virtual router.

The optional **delay minimum** keyword with the *seconds* argument specifies the number of seconds that the switch waits before issuing an advertisement claiming primary ownership. The default delay is 0 seconds. The range is from 0 to 3600 seconds.

Default	Enabled with default delay value of 0.
Format	<code>preempt [delay minimum seconds]</code>
Mode	VRRPv3 Config

no preempt (VRRPv3 Config mode)

This command prevents the switch from taking over as the primary virtual router for a VRRP group if the switch has a higher priority than the current primary virtual router.

Format	<code>no preempt</code>
Mode	VRRPv3 Config

accept-mode (VRRPv3 Config mode)

M4350

This command lets a virtual router that functions as the primary virtual router accept packets that are addressed to the address owner's virtual IP address if the virtual router is not owner of the virtual IP address.

Default	Disabled
Format	<code>accept-mode</code>
Mode	VRRPv3 Config

no accept-mode (VRRPv3 Config mode)

This command prevents a virtual router that functions as the primary virtual router from accepting packets that are addressed to the address owner's virtual IP address if the virtual router is not owner of the virtual IP address.

Format	<code>no accept-mode</code>
Mode	VRRPv3 Config

priority (VRRPv3 Config mode)

M4350

This command sets the priority level of the switch within a VRRPv3 group. The priority level controls which device becomes the primary virtual router. The range is from 1 to 254. The default is 100.

Default	100
Format	<code>priority level</code>
Mode	VRRPv3 Config

no priority (VRRPv3 Config mode)

This command sets the priority level of the switch within a VRRPv3 group to the default value of 100.

Format	<code>no priority</code>
Mode	VRRPv3 Config

timers advertize (VRRPv3 Config mode)

M4350

This command configures the interval between successive advertisements by the primary virtual router in a VRRP group.

The advertisements that are sent by the primary virtual router communicate the advertisement interval, state, and priority of the current primary virtual router. The VRRP **timers advertize** command configures the time between successive advertisement packets and the time before other routers declare the primary router to be down. VRRP backup routers learn timer values from the primary router advertisements. The timers configured on the primary router always override any other timer settings that are used for calculating the primary down time interval on VRRP backup routers. The range is from 1 to 4095 centiseconds.

Default	100
Format	<code>timers advertize centiseconds</code>
Mode	VRRPv3 Config

no timers advertize (VRRPv3 Config mode)

This command sets the timers advertize interval within a VRRPv3 group to the default value of 100 centiseconds.

Format	<code>no timers advertize</code>
Mode	VRRPv3 Config

address (VRRPv3 Config mode)

M4350

This command sets the primary or secondary IP address of the switch within a VRRPv3 group.

If you do not specify the primary or secondary option, the specified IP address is set as the primary IP address. The virtual IPv6 primary address must be a link-local address.

VRRPv3 for IPv6 requires that a primary virtual link-local IPv6 address is configured to allow the group to operate. After the primary link-local IPv6 address is established for the group, you can add the secondary global addresses.

Default	100
Format	<code>address ip-address [primary secondary]</code>
Mode	VRRPv3 Config

no address (VRRPv3 Config mode)

This command removes the configured secondary IPv4 or IPv6 address. You cannot remove the primary address, but you can modify it.

Format	no timers advertize

Mode	VRRPv3 Config

shutdown (VRRPv3 Config mode)

M4350

This command disables the VRRPv3 group configuration.

Default	100

Format	shutdown

Mode	VRRPv3 Config

no shutdown (VRRPv3 Config mode)

This command updates the virtual router state after you complete the configuration.

Format	no shutdown

Mode	VRRPv3 Config

track interface (VRRPv3 Config mode)

M4350

This command configures tracking of the interface for the switch within a VRRPv3 group. Configure Bidirectional Forwarding Detection (BFD) by using the **bfdneighbor** keyword and *ip-address* argument to track the reachability to the uplink next hop address.

After you configure interface tracking, the switch receives notifications when the state of the interface changes. If BFD tracking is enabled, a BFD session is created with the BFD destination IP address of the configured BFD neighbor IP address, and the switch receives notification when the BFD session state changes.

Use the **decrement** keyword and *number* argument to decrease the priority of the switch within the VRRPv3 group by the specified value when the interface goes down, or the associated BFD session goes down. Similarly, the priority is increased by the same specified value when the interface comes up or the associated BFD session comes up. If you do not specify the decrement value, the default decrement value used is 10.

The overall state of a track interface is considered as up only when both of the events (the “interface up event” and the “BFD session up event”) are received. The decrement or increment of the priority is based on the overall state of the tracked interface.

Default	Enabled Decrement value: 10
Format	<code>track interface {unit/slot/port vlan vlan-id} [bfdneighbor ip-address] [decrement number]</code>
Mode	VRRPv3 Config
Parameter	Definition
<i>unit/slot/port</i>	The interface that must be tracked.
<i>vlan vlan-id</i>	The VLAN ID that must be tracked.
<i>bfdneighbor ip-address</i>	The IPv4 or IPv6 address of the BFD neighbor that must be tracked.
<i>decrement number</i>	The VRRP priority decrement for the tracked interface. The range is from 1 to 254.

Command example:

```
(NETGEAR Switch) (config-if-vrrp)#track interface 1/0/6 bfdneighbor 19.168.2.99 decrement 76
```

`no track interface` (VRRPv3 Config mode)

This command disables tracking of the interface for the device within a VRRPv3 group.

Format	<code>no track interface {unit/slot/port vlan vlan-id} [bfdneighbor ip-address] [decrement]</code>
Mode	VRRPv3 Config

`track ip route` (VRRPv3 Config mode)

M4350

This command configured tracking of the IP route for the switch in a VRRPv3 group. After you configure interface tracking, the switch receives notifications when the state of the IP route changes. The decrement option can be set to decrease the priority of the device within a VRRPv3 group by the specified value when the route becomes unavailable.

Use the **decrement** keyword and *number* argument to decrease the priority of the switch within the VRRPv3 group by the specified value when the IP route goes down. Similarly, the priority is increased by the same specified value when the IP route comes up. If you do not specify the decrement value, the default decrement value used is 10.

Default	Disabled Decrement value: 10

Format	<code>track ip route <i>ip-address/prefix-len</i> [decrement <i>number</i>]</code>

Mode	VRRPv3 Config

Parameter	Definition
<i>ip-address/prefix-len</i>	The prefix and prefix length of the route to be tracked.
decrement <i>number</i>	The VRRP priority decrement for the tracked interface. The range is from 1 to 254.

no track ip route (VRRPv3 Config mode)

This command disables tracking of the route for the device within a VRRPv3 group.

Format	<code>no track ip route <i>ip-address/prefix-len</i> [decrement]</code>

Mode	VRRPv3 Config

show vrrp

M4350

Without the optional parameters, this command displays information for all active VRRPv3 groups. With parameters, this command display information for all active VRRPv3 groups configured in an IPv4 or IPv6 address family, or the active VRRPv3 groups configured in an IPv4 or IPv6 address family for the specified interface.

Format	<code>show vrrp [{<i>ipv4</i> <i>ipv6</i>}] [{<i>unit/slot/port</i> <i>vlan vlan-id</i>} <i>vr-id</i>]</code>

Mode	Privileged Config

Parameter	Definition
<i>ipv4</i>	(Optional) Indicates that the virtual router group belongs to an IPv4 address family.
<i>ipv6</i>	(Optional) Indicates that the virtual router group belongs to an IPv6 address family.
<i>unit/slot/port</i>	(Optional) The interface number to which the virtual router belongs.
<i>vlan vlan-id</i>	(Optional) The VLAN ID to which the virtual router belongs.
<i>vr-id</i>	(Optional) The virtual router group number, which can be in the range is from 1 to 255.

Command example:

The following example shows the command output when no parameters are specified.

```
(NETGEAR Switch)#show vrrp
```

```
Admin Mode..... Enable
```

```
1/0/2 - VRID 1 - Address-Family IPv4
```

```
Virtual IP address..... 1.1.1.9
Secondary IP Address(es)..... 1.1.1.4
..... 1.1.1.5
..... 1.1.1.6
Virtual MAC Address..... 00:00:5e:00:01:01
Priority..... 0
Configured Priority..... 111
Advertisement Interval..... 120 centisec
Pre-empt Mode..... Enable
Accept Mode..... Enable
Administrative Mode..... Enable
State..... Initialized
Master Router IP / Priority..... 1.1.1.3 (local) / 100
Master Advertisement interval..... 120 centisec
Master Down interval..... 360 centisec
```

```
Track Interface State DecrementPriority BFD-Neighbor
```

```
-----
1/0/9          Down  222      23.10.8.6
```

```
Track Route(pfx/len)  Reachable  DecrementPriority
```

```
-----
14.14.14.0/24        True      14
```

```
1/0/3 - VRID 2 - Address-Family IPv4
```

```
Virtual IP address..... 3.3.2.9
Secondary IP Address(es)..... 3.3.2.4
..... 3.3.2.5
..... 3.3.2.6
Virtual MAC Address..... 00:00:5e:00:01:06
Priority..... 0
Configured Priority..... 130
Advertisement Interval..... 120 centisec
Pre-empt Mode..... Enable
```

Fully Managed Switches M4250 and M4350 Series

```
Accept Mode..... Enable
Administrative Mode..... Enable
State..... Initialized
Master Router IP / Priority..... 1.1.1.3 (local) / 100
Master Advertisement interval..... 120 centisec
Master Down interval..... 360 centisec
```

```
Track Interface State DecrementPriority BFD-Neighbor
-----
```

Interface	State	Decrement	Priority	BFD-Neighbor
1/0/7	Down	125	55.16.27.8	

```
Track Route(pfx/len) Reachable DecrementPriority
-----
```

Route	Reachable	Decrement	Priority
14.14.14.0/24	True	30	

1/0/12 - VRID 3 - Address-Family IPv6

```
Virtual IP address..... 4001::2
Secondary IP Address(es)..... 4001::5
..... 4001::6
..... 4001::7
Virtual MAC Address..... 00:00:5e:00:01:06
Priority..... 0
Configured Priority..... 130
Advertisement Interval..... 120 centisec
Pre-empt Mode..... Enable
Accept Mode..... Enable
Administrative Mode..... Enable
State..... Initialized
Master Router IP / Priority..... 4001::3 (local) / 100
Master Advertisement interval..... 120 centisec
Master Down interval..... 360 centisec
```

```
Track Interface State DecrementPriority BFD-Neighbor
-----
```

Interface	State	Decrement	Priority	BFD-Neighbor
1/0/2	Down	250	5001::3	

```
Track Route(pfx/len) Reachable DecrementPriority
-----
```

Route	Reachable	Decrement	Priority
4004::3/32	True	20	

Command example:

The following example shows the command output when the **ipv4** parameter is specified.

```
(NETGEAR Switch)#show vrrp ipv4
```

```
Admin Mode..... Enable

1/0/2 - VRID 1 - Address-Family IPv4

Virtual IP address..... 1.1.1.9
Secondary IP Address(es)..... 1.1.1.4
..... 1.1.1.5
..... 1.1.1.6
Virtual MAC Address..... 00:00:5e:00:01:01
Priority..... 0
Configured Priority..... 111
Advertisement Interval..... 120 centisec
Pre-empt Mode..... Enable
Accept Mode..... Enable
Administrative Mode..... Enable
State..... Initialized
Master Router IP / Priority..... 1.1.1.3 (local) / 100
Master Advertisement interval..... 120 centisec
Master Down interval..... 360 centisec

Track Interface State DecrementPriority
-----
1/0/9          Down  222

Track Route(pfx/len)  Reachable  DecrementPriority
-----
14.14.14.0/24        True      14

1/0/3 - VRID 2 - Address-Family IPv4

Virtual IP address..... 3.3.2.9
Secondary IP Address(es)..... 3.3.2.4
..... 3.3.2.5
..... 3.3.2.6
Virtual MAC Address..... 00:00:5e:00:01:06
Priority..... 0
Configured Priority..... 130
Advertisement Interval..... 120 centisec
Pre-empt Mode..... Enable
Accept Mode..... Enable
```


Fully Managed Switches M4250 and M4350 Series

```
Administrative Mode..... Enable
State..... Initialized
Master Router IP / Priority..... 1.1.1.3 (local) / 100
Master Advertisement interval..... 120 centisecsec
Master Down interval..... 360
```

```
Track Interface State DecrementPriority
```

```
-----
1/0/7          Down  125
```

```
Track Route(pfx/len)  Reachable  DecrementPriority
```

```
-----
14.14.14.0/24        True       30
```

Command example:

The following example shows the command output when the **ipv6** parameter is specified.

```
(NETGEAR Switch)#show vrrp ipv6
```

```
Admin Mode..... Enable
```

```
1/0/2 - VRID 1 - Address-Family IPv6
```

```
Virtual IP address..... 1001::8
Secondary IP Address(es)..... 1001::5
..... 1001::6
..... 1001::7
Virtual MAC Address..... 00:00:5e:00:01:01
Priority..... 0
Configured Priority..... 100
Advertisement Interval..... 100 centisec
Pre-empt Mode..... Enable
Accept Mode..... Enable
Administrative Mode..... Enable
State..... Initialized
Master Router IP / Priority..... 1001::1 (local) / 100
Master Advertisement interval..... 100 centisec
Master Down interval..... 300 centisec
```

```
Track Interface State DecrementPriority
```

```
-----
1/0/9          Down  222
```

```
Track Route(pfx/len)  Reachable  DecrementPriority
```

```
-----
2001::2/32        True       14
```

1/0/12 - VRID 3 - Address-Family IPv6

```

Virtual IP address..... 4001::2
Secondary IP Address(es)..... 4001::5
..... 4001::6
..... 4001::7
Virtual MAC Address..... 00:00:5e:00:01:06
Priority..... 130
Configured Priority..... 130
Advertisement Interval..... 120 centisec
Pre-empt Mode..... Enable
Accept Mode..... Enable
Administrative Mode..... Enable
State..... Master
Master Router IP / Priority..... 4001::3 (local) / 130
Master Advertisement interval..... 120 centisec
Master Down interval..... 360 centisec

```

Track Interface State DecrementPriority

```

-----
1/0/24          Down  320

```

Track Route(pfx/len) Reachable DecrementPriority

```

-----
7003::4/32          True          50

```

Command example:

The following example shows the command output when the **ipv4** parameter, an interface, and a virtual router group number is specified.

(NETGEAR Switch)#show vrrp ipv4 1/0/3 1

```

Virtual IP address..... 1.1.1.9
Secondary IP Address(es)..... 1.1.1.4
..... 1.1.1.5
..... 1.1.1.6
Virtual MAC Address..... 00:00:5e:00:01:01
Priority..... 0
Configured Priority..... 111
Advertisement Interval..... 222 centisec
Pre-empt Mode..... Enable
Accept Mode..... Enable
Administrative Mode..... Enable
State..... Initialized

```

Fully Managed Switches M4250 and M4350 Series

```
Master Router IP / Priority..... 1.1.1.3 (local) / 100
Master Advertisement interval..... 1000 centisec
Master Down interval..... 3000 centisec
```

```
Track Interface State Decrement-Priority
```

```
-----
0/9          Down  222
```

```
Track Route(pfx/len)  Reachable  Decrement-Priority
```

```
-----
14.14.14.0/24        True       14
```

show vrrp brief

M4350

This command displays brief information for all active VRRPv3 groups.

Format show vrrp brief

Mode Privileged Config

Field	Description
Interface	The interface on which VRRP is configured.
VR	The ID of the virtual router.
A-F	The IP address family type (IPv4 or IPv6) to which the virtual router belongs.
Pri	The priority range of the virtual router.
AdvIntvl	The advertisement interval configured for the virtual router.
Pre	The preemption state of the virtual router.
Acc	The accept mode of the virtual router.
State	The VRRP group state. The state can be one of the following: Init, Backup (now referred to as secondary), or Master (now referred to as primary).
VR IP address	The virtual IP address for the VRRP group.

Command example:

```
(NETGEAR Switch)#show vrrp brief
Interface  VRID A-F  Pri AdvIntvl Pre Acc State  VR IP Address
-----
0/1        1   IPv4 100 200s    Y  Y  Init   192.0.1.10
0/3        2   IPv4 200 200s    Y  Y  Init   124.0.3.17
0/1        7   IPv6 100 200s    Y  Y  Backup 5002::1
0/5        2   IPV6 20  200s    Y  Y  Master 2001::2
```

show vrrp statistics

M4350

Without the optional parameters, this command displays information for all active VRRPv3 groups. With parameters, this command display information for all active VRRPv3 groups configured in an IPv4 or IPv6 address family, or the active VRRPv3 groups configured in an IPv4 or IPv6 address family for the specified interface.

Format	show vrrp statistics [{ipv4 ipv6}] [{unit/slot/port vlan vlan-id} vr-id]
Mode	Privileged Config
Parameter	Definition
ipv4	(Optional) Indicates that the virtual router group belongs to an IPv4 address family.
ipv6	(Optional) Indicates that the virtual router group belongs to an IPv6 address family.
unit/slot/port	(Optional) The interface number to which the virtual router belongs.
vlan vlan-id	(Optional) The VLAN ID to which the virtual router belongs.
vr-id	(Optional) The virtual router group number, which can be in the range is from 1 to 255.

Command example:

The following example shows the command output when no parameters are specified.

```
(NETGEAR Switch)#show vrrp statistics
```

```
Router Checksum Errors..... 2
Router Version Errors..... 3
Router VRID Errors..... 4
Global Statistics Discontinuity Time..... 0 days 0 hrs 0 mins 0 secs
```

Command example:

The following example shows the command output when the **ipv6** parameter, an interface, and a virtual router group number is specified.

```
(NETGEAR Switch)#show vrrp statistics ipv6 1/0/1 2
```

```
Master Transitions..... 2
New Master Reason..... Priority
Advertisements Received..... 64
Advertisements Sent..... 12
Advertisement Interval Errors..... 0
IP TTL Errors..... 1
Last Protocol Error Reason..... Version Error
Zero Priority Packets Received..... 0
Zero Priority Packets Sent..... 1
```

```

Invalid Type Packets Received..... 0
Address List Errors..... 2
Packet Length Errors..... 4
Row Discontinuity Time..... 0 days 0 hrs 0 mins 0 secs
Refresh Rate (in milliseconds)..... 0

```

clear vrrp statistics

M4350

Use this command to clear VRRP statistical information for a specific interface or VLAN within a VRRPv3 group and IP address family. If you enter this command the optional arguments, the global statistics and all virtual routers (both IPv4 and IPv6) are reset.

If you specify the optional arguments, the statistics are reset for the virtual router that corresponds to the specified combination of the IP address family, interface or VLAN, and VR ID.

Format	clear vrrp statistics [{ipv4 ipv6} {unit/slot/port vlan vlan-id} vrid]
Modes	Privileged Config
Term	Definition
ipv4	(Optional) Indicates that the virtual router group belongs to an IPv4 address family.
ipv6	(Optional) Indicates that the virtual router group belongs to an IPv6 address family.
unit/slot/port	(Optional) The interface number to which the virtual router belongs.
vlan vlan-id	(Optional) The VLAN ID to which the virtual router belongs.
vr-id	(Optional) The virtual router group number, which can be in the range is from 1 to 255.

DHCP and BootP Relay Commands

This section describes the commands you use to configure BootP/DHCP Relay on the switch. A DHCP relay agent operates at Layer 3 and forwards DHCP requests and replies between clients and servers when they are not on the same physical subnet.

bootpdhcprelay cidoptmode

M4250**M4350**

This command enables the circuit ID option mode for BootP/DHCP Relay on the system.

Default	disabled
Format	bootpdhcprelay cidoptmode
Mode	Global Config

no bootpdhcprelay cidoptmode

This command disables the circuit ID option mode for BootP/DHCP Relay on the system.

Format	no bootpdhcprelay cidoptmode
Mode	Global Config

bootpdhcprelay maxhopcount

M4250**M4350**

This command configures the maximum allowable relay agent hops for BootP/DHCP Relay on the system. The *hops* parameter has a range of 1 to 16.

Default	4
Format	bootpdhcprelay maxhopcount hops
Mode	Global Config

no bootpdhcprelay maxhopcount

This command configures the default maximum allowable relay agent hops for BootP/DHCP Relay on the system.

Format	no bootpdhcprelay maxhopcount
Mode	Global Config

bootpdhcprelay minwaittime

M4250**M4350**

This command configures the minimum wait time in seconds for the BootP/DHCP Relay on the switch. When the BootP relay agent receives a BOOTREQUEST message, it can use the

seconds-since-client-began-booting field of the request as a factor in deciding whether to relay the request or not. The **minwaittime** *seconds* parameter has a range of 0 to 100 seconds.

Default	0
Format	bootpdhcprelay minwaittime <i>seconds</i>
Mode	Global Config

no bootpdhcprelay minwaittime

This command resets the minimum wait time to the default for the BootP/DHCP Relay on the switch.

Format	no bootpdhcprelay minwaittime
Mode	Global Config

bootpdhcprelay server-override

M4250

M4350

This command enables the addition of suboption 5 (link selection) and suboption 11 (server ID override) in option 82 of the DHCP packet that is received from a DHCP client. You can use the command in both Global Config mode and Interface Config mode.

When you enter the command in Global Config mode, the server override is globally enabled, and the feature is then enabled on all routing interfaces. A DHCP packet that is received from a DHCP client has suboption 5 and suboption 11 for option 82 added to the packet.

When this command is issued in Interface Config mode, server-override is enabled for that interface only.

Default	Disabled globally and on all interfaces
Format	bootpdhcprelay server-override
Mode	Global Config Interface Config

Command example:

```
(NETGEAR Switch) (Config)# bootpdhcprelay server-override
```

Command example:

```
(NETGEAR Switch) (Config)#interface 0/26
(NETGEAR Switch) (Interface 0/26)#bootpdhcprelay server-override
```

no bootpdhcprelay server-override

This command disables the server-override feature

Format	no bootpdhcprelay server-override
Mode	Global Config Interface Config

bootpdhcprelay source-interface

M4250

M4350

This command sets the source interface for a routing interface, and uses the interface to get the relay agent IP address. You can use this command to specify an interface for which the IP address is passed as a relay agent IP address. In Global Config mode, the source interface is set globally. In Interface Config mode, the source interface is set for the specified interface.

If the source interface is set in Interface Config mode, that value takes precedence over the globally set value.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Default	Disabled is disabled globally and on all interfaces
Format	bootpdhcprelay source-interface interface { <i>unit/slot/port</i> <i>vlan vlanid</i> <i>loopback loopbackid</i> >}
Mode	Global Config Interface Config

Command example:

```
(NETGEAR Switch) (Config)# bootpdhcprelay source-interface interface vlan 10
```

Command example:

```
(NETGEAR Switch) (Config)#interface 0/26
(NETGEAR Switch) (Interface 0/26)#bootpdhcprelay source-interface interface vlan 10
```


no bootpdhcprelay server-override

This command disables the source interface feature globally and clears all source interface entries.

Format	no bootpdhcprelay source-interface

Mode	Global Config Interface Config

show bootpdhcprelay

M4250

M4350

This command displays all BootP/DHCP relay information, or the BootP/DHCP relay information for a specific interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show bootpdhcprelay [interface <i>unit/slot/port</i>]

Modes	Privileged EXEC User EXEC

Term	Definition
Maximum Hop Count	The maximum allowable relay agent hops.
Minimum Wait Time (Seconds)	The minimum wait time.
Admin Mode	Indicates whether the relaying of requests is enabled or disabled.
Circuit Id Option Mode	The DHCP circuit Id option, which can be enabled or disabled.
Server Override Mode	The DHCP server override mode, which can be enabled or disabled.
Source Interface	The DHCP source interface, which can be enabled or disabled.

Command example:

```
(NETGEAR Switch)#show bootpdhcprelay
```

```
Maximum Hop Count..... 4
Minimum Wait Time(Seconds)..... 0
Admin Mode..... Disable
Circuit Id option mode..... Disable
Server Override Mode..... Disable
Source Interface..... Disable
```

IP Helper Commands

This section describes the commands to configure and monitor the IP Helper agent. IP Helper relays DHCP and other broadcast UDP packets from a local client to one or more servers which are not on the same network at the client.

The IP Helper feature provides a mechanism that allows a router to forward certain configured UDP broadcast packets to a particular IP address. This allows various applications to reach servers on nonlocal subnets, even if the application was designed to assume a server is always on a local subnet and uses broadcast packets (with either the limited broadcast address 255.255.255.255, or a network directed broadcast address) to reach the server.

The network administrator can configure relay entries both globally and on routing interfaces. Each relay entry maps an ingress interface and destination UDP port number to a single IPv4 address (the helper address). The network administrator may configure multiple relay entries for the same interface and UDP port, in which case the relay agent relays matching packets to each server address. Interface configuration takes priority over global configuration. That is, if a packet's destination UDP port matches any entry on the ingress interface, the packet is handled according to the interface configuration. If the packet does not match any entry on the ingress interface, the packet is handled according to the global IP helper configuration.

The network administrator can configure discard relay entries, which direct the system to discard matching packets. Discard entries are used to discard packets received on a specific interface when those packets would otherwise be relayed according to a global relay entry. Discard relay entries may be configured on interfaces, but are not configured globally.

In addition to configuring the server addresses, the network administrator also configures which UDP ports are forwarded. Certain UDP port numbers can be specified by name in the UI as a convenience, but the network administrator can configure a relay entry with any UDP port number. The network administrator may configure relay entries that do not specify a destination UDP port. The relay agent relays assumes these entries match packets with the UDP destination ports listed in the following table. This is the list of default ports.

Table 9. Default ports—UDP port numbers implied by wildcard

Protocol	UDP Port Number
IEN-116 Name Service	42
DNS	53
NetBIOS Name Server	137
NetBIOS Datagram Server	138
TACACS Server	49
Time Service	37

Table 9. Default ports—UDP port numbers implied by wildcard (continued)

Protocol	UDP Port Number
DHCP	67
Trivial File Transfer Protocol (TFTP)	69

The system limits the number of relay entries to four times the maximum number of routing interfaces. The network administrator can allocate the relay entries as he likes. There is no limit to the number of relay entries on an individual interface, and no limit to the number of servers for an interface and UDP port pair.

The relay agent relays DHCP packets in both directions. It relays broadcast packets from the client to one or more DHCP servers, and relays to the client packets that the DHCP server unicasts back to the relay agent. For other protocols, the relay agent only relays broadcast packets from the client to the server. Packets from the server back to the client are assumed to be unicast directly to the client. Because there is no relay in the return direction for protocols other than DHCP, the relay agent retains the source IP address from the original client packet. The relay agent uses a local IP address as the source IP address of relayed DHCP client packets.

When a switch receives a broadcast UDP packet on a routing interface, the relay agent checks if the interface is configured to relay the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise, the relay agent checks if there is a global configuration for the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise the packet is not relayed. Note that if the packet matches a discard relay entry on the ingress interface, then the packet is not forwarded, regardless of the global configuration.

The relay agent only relays packets that meet the following conditions:

- The destination MAC address must be the all-ones broadcast address (FF:FF:FF:FF:FF:FF)
- The destination IP address must be the limited broadcast address (255.255.255.255) or a directed broadcast address for the receive interface.
- The IP time-to-live (TTL) must be greater than 1.
- The protocol field in the IP header must be UDP (17).
- The destination UDP port must match a configured relay entry.

ip helper-address (Global Config)

M4250

M4350

Use this command to configure the relay of certain UDP broadcast packets received on any interface. This command can be invoked multiple times, either to specify multiple server addresses for a specified UDP port number or to specify multiple UDP port numbers handled by a specific server.

Default	No helper addresses are configured.
Format	<code>ip helper-address server-address [dest-udp-port dhcp domain isakmp mobile-ip nameserver netbios-dgm netbios-ns ntp pim-auto-rp rip tacacs tftp time]</code>
Mode	Global Config

Parameter	Description
server-address	The IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be an IP address configured on any interface of the local router.
dest-udp-port	A destination UDP port number from 0 to 65535.
port-name	As an option, you can specify the destination UDP port by its name. Whether you specify a port by its number or its name does not matter for the configuration. The names recognized are as follows: • dhcp (port 67) • domain (port 53) • isakmp (port 500) • mobile-ip (port 434) • nameserver (port 42) • netbios-dgm (port 138) • netbios-ns (port 137) • ntp (port 123) • pim-auto-rp (port 496) • rip (port 520) • tacacs (port 49) • tftp (port 69) • time (port 37) Other ports must be specified by number.

Command example:

The following example relays DHCP packets that are received on any interface to two DHCP servers, 10.1.1.1 and 10.1.2.1:

```
(NETGEAR Switch)#config
(NETGEAR Switch)(config)#ip helper-address 10.1.1.1 dhcp
(NETGEAR Switch)(config)#ip helper-address 10.1.2.1 dhcp
```

Command example:

The following example relays UDP packets that are received on any interface for all default ports to the server at 20.1.1.1:

```
(NETGEAR Switch)#config
(NETGEAR Switch)(config)#ip helper-address 20.1.1.1
```

no ip helper-address (Global Config)

Use the **no ip helper-address** command to delete an IP helper entry. Use the command without any arguments to clear all global IP helper addresses.

Format	no ip helper-address [<i>server-address</i>] [<i>dest-udp-port</i> dhcp domain isakmp mobile-ip nameserver netbios-dgm netbios-ns ntp pim-auto-rp rip tacacs tftp time]

Mode	Global Config

ip helper-address (Interface Config)

M4250**M4350**

Use this command to configure the relay of certain UDP broadcast packets received on a specific interface or range of interfaces. This command can be invoked multiple times on a routing interface, either to specify multiple server addresses for a specified port number or to specify multiple port numbers handled by a specific server.

Default	No helper addresses are configured.

Format	ip helper-address { <i>server-address</i> discard} [<i>dest-udp-port</i> dhcp domain isakmp mobile ip nameserver netbios-dgm netbios-ns ntp pim-auto-rp rip tacacs tftp time]

Mode	Interface Config

Parameter	Description
server-address	The IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be in a subnet on the interface where the relay entry is configured, and cannot be an IP address configured on any interface of the local router.
discard	Matching packets should be discarded rather than relayed, even if a global ip helper-address configuration matches the packet.
dest-udp-port	A destination UDP port number from 0 to 65535.

Parameter	Description
port-name	As an option, you can specify the destination UDP port by its name. Whether you specify a port by its number or its name does not matter for the configuration. The names recognized are as follows: • dhcp (port 67) • domain (port 53) • isakmp (port 500) • mobile-ip (port 434) • nameserver (port 42) • netbios-dgm (port 138) • netbios-ns (port 137) • ntp (port 123) • pim-auto-rp (port 496) • rip (port 520) • tacacs (port 49) • tftp (port 69) • time (port 37) Other ports must be specified by number.

Command example:

The following example relays DHCP packets that are received on interface 1/0/2 to two DHCP servers, 192.168.10.1 and 192.168.20.1:

```
(NETGEAR Switch)#config
(NETGEAR Switch)(config)#interface 1/0/2
(NETGEAR Switch)(interface 1/0/2)#ip helper-address 192.168.10.1 dhcp
(NETGEAR Switch)(interface 1/0/2)#ip helper-address 192.168.20.1 dhcp
```

Command example:

The following example relays DHCP and DNS packets to 192.168.30.1:

```
(NETGEAR Switch)#config
(NETGEAR Switch)(config)#interface 1/0/2
(NETGEAR Switch)(interface 1/0/2)#ip helper-address 192.168.30.1 dhcp
(NETGEAR Switch)(interface 1/0/2)#ip helper-address 192.168.30.1 dns
```

Command example:

The following example takes precedence over the **ip helper-address** command that you enter in global configuration mode. With the following configuration, the relay agent relays DHCP packets that are received on any interface other than 1/0/2 and 1/0/17 to 192.168.40.1, relays DHCP and DNS packets that are received on 1/0/2 to 192.168.40.2, relays SNMP traps (port 162) that are received on interface 1/0/17 to 192.168.23.1, and drops DHCP packets that are received on 1/0/17:

```
(NETGEAR Switch)#config
(NETGEAR Switch)(config)#ip helper-address 192.168.40.1 dhcp
(NETGEAR Switch)(config)#interface 1/0/2
```

Fully Managed Switches M4250 and M4350 Series

```
(NETGEAR Switch) (interface 1/0/2) #ip helper-address 192.168.40.2 dhcp
(NETGEAR Switch) (interface 1/0/2) #ip helper-address 192.168.40.2 domain
(NETGEAR Switch) (interface 1/0/2) #exit
(NETGEAR Switch) (config) #interface 1/0/17
(NETGEAR Switch) (interface 1/0/17) #ip helper-address 192.168.23.1 162
(NETGEAR Switch) (interface 1/0/17) #ip helper-address discard dhcp
```

no ip helper-address (Interface Config)

Use this command to delete a relay entry on an interface. The command without any arguments clears all helper addresses on the interface.

Format	no ip helper-address [<i>server-address</i> discard] [<i>dest-udp-port</i> dhcp domain isakmp mobile ip nameserver netbios-dgm netbios-ns ntp pim-auto-rp rip tacacs tftp time]

Mode	Interface Config

ip helper enable

M4250

M4350

Use this command to enable relay of UDP packets. This command can be used to temporarily disable IP helper without deleting all IP helper addresses. This command replaces the **bootpdhcrelay enable** command, but affects not only relay of DHCP packets, but also relay of any other protocols for which an IP helper address has been configured.

Default	disabled
Format	ip helper enable

Mode	Global Config

Command example:

```
(NETGEAR Switch) (config) #ip helper enable
```

no ip helper enable

Use the no form of this command to disable relay of all UDP packets.

Format	no ip helper enable

Mode	Global Config

show ip helper-address

M4250

M4350

Use this command to display the IP helper address configuration.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* can be a number from 1–4093.

Format	show ip helper-address [<i>unit/slot/port</i> vlan <i>vlan-id</i>]
Mode	Privileged EXEC
Parameter	Description
interface	The relay configuration is applied to packets that arrive on this interface. This field is set to <i>any</i> for global IP helper entries.
UDP Port	The relay configuration is applied to packets whose destination UDP port is this port. Entries whose UDP port is identified as <i>any</i> are applied to packets with the destination UDP ports listed in Table 4.
Discard	If Yes, packets arriving on the interface with the specified destination UDP port are discarded rather than relayed. Discard entries are used to override global IP helper address entries which otherwise might apply to a packet.
Hit Count	The number of times the IP helper entry has been used to relay or discard a packet.
Server Address	The IPv4 address of the server to which packets are relayed.

Command example:

```
(NETGEAR Switch) #show ip helper-address
```

IP helper is enabled

Interface	UDP Port	Discard	Hit Count	Server Address
-----	-----	-----	-----	-----
1/0/1	dhcp	No	10	10.100.1.254
1/0/17	any	Yes	2	10.100.2.254

show ip helper statistics

M4250

M4350

Use this command to display the number of DHCP and other UDP packets processed and relayed by the UDP relay agent.

Format	show ip helper statistics	
Mode	Privileged EXEC	
Parameter	Description	
DHCP client messages received	The number of valid messages received from a DHCP client. The count is only incremented if IP helper is enabled globally, the ingress routing interface is up, and the packet passes a number of validity checks, such as having a TTL>1 and having valid source and destination IP addresses.	
DHCP client messages relayed	The number of DHCP client messages relayed to a server. If a message is relayed to multiple servers, the count is incremented once for each server.	
DHCP server messages received	The number of DHCP responses received from the DHCP server. This count only includes messages that the DHCP server unicasts to the relay agent for relay to the client.	
DHCP server messages relayed	The number of DHCP server messages relayed to a client.	
UDP clients messages received	The number of valid UDP packets received. This count includes DHCP messages and all other protocols relayed. Conditions are similar to those for the first statistic in this table.	
UDP clients messages relayed	The number of UDP packets relayed. This count includes DHCP messages relayed as well as all other protocols. The count is incremented for each server to which a packet is sent.	
DHCP message hop count exceeded max	The number of DHCP client messages received whose hop count is larger than the maximum allowed. The maximum hop count is a configurable value listed in show bootpdhcrelay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.	
DHCP message with secs field below min	The number of DHCP client messages received whose secs field is less than the minimum value. The minimum secs value is a configurable value and is displayed in show bootpdhcrelay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.	
DHCP message with giaddr set to local address	The number of DHCP client messages received whose gateway address, giaddr, is already set to an IP address configured on one of the relay agent's own IP addresses. In this case, another device is attempting to spoof the relay agent's address. The relay agent does not relay such packets. A log message gives details for each occurrence.	
Packets with expired TTL	The number of packets received with TTL of 0 or 1 that might otherwise have been relayed.	
Packets that matched a discard entry	The number of packets ignored by the relay agent because they match a discard relay entry.	

Command example:

```
(NETGEAR Switch)#show ip helper statistics
DHCP client messages received..... 8
DHCP client messages relayed..... 2
DHCP server messages received..... 2
DHCP server messages relayed..... 2
UDP client messages received..... 8
UDP client messages relayed..... 2
DHCP message hop count exceeded max..... 0
DHCP message with secs field below min..... 0
DHCP message with giaddr set to local address.. 0
Packets with expired TTL..... 0
Packets that matched a discard entry..... 0
```

clear ip helper statistics

M4250

M4350

Use this command to reset to zero the statistics displayed in the output of the **show ip helper statistics** command.

Format	clear ip helper statistics
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #clear ip helper statistics
```

Open Shortest Path First commands

Note: Open Shortest Path First (OSPF) commands are supported on the M4350 series switches only. The M4250 series switches do not support OSPF.

This section describes the commands you use to view and configure Open Shortest Path First (OSPF), which is a link-state routing protocol that you use to route traffic within a network. This section contains the following subsections:

- [General OSPF Commands on page 1013](#)
- [OSPF Interface Commands on page 1036](#)

- [OSPF Graceful Restart Commands on page 1043](#)
- [OSPFv2 Stub Router Commands on page 1046](#)
- [OSPF Show Commands on page 1048](#)

General OSPF Commands

Note: Open Shortest Path First (OSPF) commands are supported on the M4350 series switches only. The M4250 series switches do not support OSPF.

router ospf

M4350

Use this command to enter Router OSPF Config mode.

Format	router ospf
Mode	Global Config

enable (Router OSPF Config)

M4350

This command enabled the administrative mode of OSPF on the switch.

Default	enabled
Format	enable
Mode	Router OSPF Config

no enable (Router OSPF Config)

This command disabled the administrative mode of OSPF on the switch.

Format	no enable
Mode	Router OSPF Config

network area (Router OSPF Config)

M4350

This command enables OSPFv2 on an interface and sets its area ID if the IP address of an interface is covered by this network command.

Default	disabled
Format	<i>network ip-address wildcard-mask area area-id</i>
Mode	Router OSPF Config

no network area (Router OSPF Config)

This command disables OSPFv2 on a interface if the IP address of an interface was earlier covered by this network command.

Format	<i>no network ip-address wildcard-mask area area-id</i>
Mode	Router OSPF Config

1583compatibility

M4350

This command enables OSPF 1583 compatibility.

Note: 1583 compatibility mode is enabled by default. If all OSPF routers in the routing domain are capable of operating according to RFC 2328, disable the OSPF 1583 compatibility mode.

Default	enabled
Format	<i>1583compatibility</i>
Mode	Router OSPF Config

no 1583compatibility (Router OSPF Config)

This command disables OSPF 1583 compatibility.

Format	<i>no 1583compatibility</i>
Mode	Router OSPF Config

area default-cost (Router OSPF Config)

M4350

This command configures the metric default cost for the stub area. For the *value* argument, you must specify an integer value between 1–16777215.

Format	<code>area <i>area-id</i> default-cost <i>value</i></code>

Mode	Router OSPF Config

no area default-cost (Router OSPF Config)

This command resets the metric default cost for the stub area.

Format	<code>no area <i>area-id</i> default-cost</code>

Mode	Router OSPF Config

area nssa (Router OSPF Config)

M4350

This command configures the specified *area-id* to function as an NSSA.

Format	<code>area <i>area-id</i> nssa</code>

Mode	Router OSPF Config

no area nssa (Router OSPF Config)

This command disables NSSA from the specified area id.

Format	<code>no area <i>area-id</i> nssa</code>

Mode	Router OSPF Config

area nssa default-info-originate (Router OSPF Config)

M4350

This command configures the metric value and type for the default route advertised into the NSSA. The optional *metric* parameter specifies the metric of the default route and must be in the range 1–16777214. If no metric is specified, the default value is ****. The metric type can be comparable (nssa-external 1) or noncomparable (nssa-external 2).

Format	<code>area <i>area-id</i> nssa default-info-originate [<i>metric</i>] [comparable non-comparable]</code>

Mode	Router OSPF Config

no area nssa default-info-originate (Router OSPF Config)

This command disables the default route advertised into the NSSA.

Format	no area <i>area-id</i> nssa default-info-originate [<i>metric</i>] [comparable non-comparable]

Mode	Router OSPF Config

area nssa no-redistribute (Router OSPF Config)

M4350

This command configures the NSSA Area Border router (ABR) so that learned external routes will not be redistributed to the NSSA.

Format	area <i>area-id</i> nssa no-redistribute

Mode	Router OSPF Config

no area nssa no-redistribute (Router OSPF Config)

This command disables the NSSA ABR so that learned external routes are redistributed to the NSSA.

Format	no area <i>area-id</i> nssa no-redistribute

Mode	Router OSPF Config

area nssa no-summary (Router OSPF Config)

M4350

This command configures the NSSA so that summary LSAs are not advertised into the NSSA.

Format	area <i>area-id</i> nssa no-summary

Mode	Router OSPF Config

no area nssa no-summary (Router OSPF Config)

This command disables nssa from the summary LSAs.

Format	no area <i>area-id</i> nssa no-summary

Mode	Router OSPF Config

area nssa translator-role (Router OSPF Config)

M4350

This command configures the translator role of the NSSA. The **always** keyword lets the switch assume the role of the translator when it becomes a border router. The **candidate** keyword lets the switch participate in the translator election process when it attains border router status.

Format	area <i>area-id</i> nssa translator-role {always candidate}

Mode	Router OSPF Config

no area nssa translator-role (Router OSPF Config)

This command disables the NSSA translator role from the specified area id.

Format	no area <i>area-id</i> nssa translator-role {always candidate}

Mode	Router OSPF Config

area nssa translator-stab-intv (Router OSPF Config)

M4350

This command configures the translator *stabilityinterval* of the NSSA. The *stabilityinterval* is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.

Format	area <i>area-id</i> nssa translator-stab-intv <i>stabilityinterval</i>

Mode	Router OSPF Config

no area nssa translator-stab-intv (Router OSPF Config)

This command disables the nssa translator's *stabilityinterval* from the specified area id.

Format	no area <i>area-id</i> nssa translator-stab-intv <i>stabilityinterval</i>

Mode	Router OSPF Config

area range (Router OSPF Config)

M4350

Use this command in Router Configuration mode to configure a summary prefix that an area border router advertises for a specific area.

Default	No area ranges are configured by default. No cost is configured by default.
Format	<code>area area-id range ip-address netmask {summarylink nssaexternallink} [advertise not-advertise] [cost cost]</code>
Mode	Router OSPF Config

Parameter	Description
area-id	The area identifier for the area whose networks are to be summarized.
prefix netmask	The summary prefix to be advertised when the ABR computes a route to one or more networks within this prefix in this area.
summarylink	The area range is used when summarizing prefixes advertised in type 3 summary LSAs.
nssaexternallink	The area range is used when translating type 7 LSAs to type 5 LSAs.
advertise	[Optional] The summary prefix is advertised when the area range is active. This is the default.
not-advertise	[Optional] Neither the summary prefix nor the contained prefixes are advertised when the area range is active. With the not-advertise option, any static cost previously configured is removed from the system configuration.
cost	[Optional] OSPF sets the metric field in the summary LSA to the configured value rather than setting the metric to the largest cost among the networks covered by the area range. A static cost may only be configured if the area range is configured to advertise the summary. The range is 0 to 16,777,215. If the cost is set to 16,777,215 for type 3 summarization, a type 3 summary LSA is not advertised, but contained networks are suppressed. This behavior is equivalent to specifying the not-advertise option. If the range is configured for type 7 to type 5 translation, a type 5 LSA is sent if the metric is set to 16,777,215; however, other routers will not compute a route from a type 5 LSA with this metric.

no area range (Router OSPF Config)

This command deletes a specified area range or reverts an option to its default.

Format	<code>no area area-id range prefix netmask {summarylink nssaexternallink} [advertise not-advertise] [cost]</code>
Mode	Router OSPF Config

Command example:

```
!! Create area range
(NETGEAR Switch) (Config-router)#area 1 range 10.0.0.0 255.0.0.0 summarylink
!! Delete area range
(NETGEAR Switch) (Config-router)#no area 1 range 10.0.0.0 255.0.0.0 summarylink
```


You can use the **no area range** command to revert the **[advertise | not-advertise]** option to its default without deleting the area range. Deleting and recreating the area range would cause OSPF to temporarily advertise the prefixes contained within the range. Note that using either the **advertise** or **not-advertise** keyword reverts the configuration to the default. For example:

```
!! Create area range. Suppress summary.
(NETGEAR Switch) (Config-router)#area 1 range 10.0.0.0 255.0.0.0 summarylink
not-advertise
!! Advertise summary.
(NETGEAR Switch) (Config-router)#no area 1 range 10.0.0.0 255.0.0.0 summarylink
not-advertise
```

You can also use the **no area range** command to remove a static area range cost, so that OSPF sets the cost to the largest cost among the contained routes.

```
!! Create area range with static cost.
(NETGEAR Switch) (Config-router)#area 1 range 10.0.0.0 255.0.0.0 summarylink cost 1000
!! Remove static cost.
(NETGEAR Switch) (Config-router)#no area 1 range 10.0.0.0 255.0.0.0 summarylink cost
```

area stub (Router OSPF Config)

M4350

This command creates a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area.

Format	<code>area area-id stub</code>

Mode	Router OSPF Config

no area stub (Router OSPF Config)

This command deletes a stub area for the specified area ID.

Format	<code>no area area-id stub</code>

Mode	Router OSPF Config

area stub no-summary (Router OSPF Config)

M4350

This command configures the Summary LSA mode for the stub area identified by *area-id*. Use this command to prevent LSA Summaries from being sent.

Default	disabled
Format	area <i>area-id</i> stub no-summary
Mode	Router OSPF Config

no area stub no-summary (Router OSPF Config)

This command configures the default Summary LSA mode for the stub area identified by *area-id*.

Format	no area <i>area-id</i> stub no-summary
Mode	Router OSPF Config

area virtual-link (Router OSPF Config)

M4350

This command creates the OSPF virtual interface for the specified *area-id* and *neighbor*. The *neighbor* parameter is the router ID of the neighbor.

Format	area <i>area-id</i> virtual-link <i>neighbor</i>
Mode	Router OSPF Config

no area virtual-link (Router OSPF Config)

This command deletes the OSPF virtual interface from the interface, identified by *area-id* and *neighbor*. The *neighbor* parameter is the router ID of the neighbor.

Format	no area <i>area-id</i> virtual-link <i>neighbor</i>
Mode	Router OSPF Config

area virtual-link authentication

M4350

This command configures the authentication type and key for the OSPF virtual interface identified by *area-id* and *neighbor*. The *neighbor* parameter is the router ID of the neighbor. The type of authentication can be either **none**, **simple**, or **encrypt**. If you select **simple** or **encrypt**, the *key* parameter is composed of standard displayable, noncontrol keystrokes from a standard 101/102-key keyboard. The authentication *key* must be 8 bytes or less if the authentication type is **simple**. If the type is **encrypt**, the *key* can be up to 16

bytes. Unauthenticated interfaces do not need an authentication key. If the type is **encrypt**, a *keyid* in the range of 0 and 255 must be specified. The default value for authentication type is **none**. Neither the default password key nor the default key id are configured.

Default	none
Format	area <i>area-id</i> virtual-link <i>neighbor</i> authentication {none simple <i>key</i> encrypt <i>key</i> <i>keyid</i> }
Mode	Router OSPF Config

no area virtual-link authentication (Router OSPF Config)

This command configures the default authentication type for the OSPF virtual interface identified by *area-id* and *neighbor*. The *neighbor* parameter is the router ID of the neighbor.

Format	no area <i>area-id</i> virtual-link <i>neighbor</i> authentication
Mode	Router OSPF Config

area virtual-link dead-interval (Router OSPF Config)

M4350

This command configures the dead interval for the OSPF virtual interface on the virtual interface identified by *area-id* and *neighbor*. The *neighbor* parameter is the router ID of the neighbor. The range for *seconds* is 1 to 65535.

Default	40
Format	area <i>area-id</i> virtual-link <i>neighbor</i> dead-interval <i>seconds</i>
Mode	Router OSPF Config

no area virtual-link dead-interval (Router OSPF Config)

This command configures the default dead interval for the OSPF virtual interface on the virtual interface identified by *area-id* and *neighbor*. The *neighbor* parameter is the router ID of the neighbor.

Format	no area <i>area-id</i> virtual-link <i>neighbor</i> dead-interval
Mode	Router OSPF Config

area virtual-link hello-interval (Router OSPF Config)

M4350

This command configures the hello interval for the OSPF virtual interface on the virtual interface identified by *area-id* and *neighbor*. The *neighbor* parameter is the router ID of the neighbor. The range for *seconds* is 1 to 65535.

Default	10
Format	<code>area area-id virtual-link neighbor hello-interval 1-65535</code>
Mode	Router OSPF Config

no area virtual-link hello-interval (Router OSPF Config)

This command configures the default hello interval for the OSPF virtual interface on the virtual interface identified by *area-id* and *neighbor*. The *neighbor* parameter is the router ID of the neighbor.

Format	<code>no area area-id virtual-link neighbor hello-interval</code>
Mode	Router OSPF Config

area virtual-link retransmit-interval (Router OSPF Config)

M4350

This command configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by *area-id* and *neighbor*. The *neighbor* parameter is the router ID of the neighbor. The range for *seconds* is 0 to 3600.

Default	5
Format	<code>area area-id virtual-link neighbor retransmit-interval seconds</code>
Mode	Router OSPF Config

no area virtual-link retransmit-interval (Router OSPF Config)

This command configures the default retransmit interval for the OSPF virtual interface on the virtual interface identified by *area-id* and *neighbor*. The *neighbor* parameter is the router ID of the neighbor.

Format	<code>no area area-id virtual-link neighbor retransmit-interval</code>
Mode	Router OSPF Config

area virtual-link transmit-delay (Router OSPF Config)

M4350

This command configures the transmit delay for the OSPF virtual interface on the virtual interface identified by *area-id* and *neighbor*. The *neighbor* parameter is the router ID of the neighbor. The range for *seconds* is 0 to 3600 (1 hour).

Default	1
Format	<code>area area-id virtual-link neighbor transmit-delay seconds</code>
Mode	Router OSPF Config

no area virtual-link transmit-delay (Router OSPF Config)

This command resets the default transmit delay for the OSPF virtual interface to the default value.

Format	<code>no area area-id virtual-link neighbor transmit-delay</code>
Mode	Router OSPF Config

auto-cost (Router OSPF Config)

M4350

By default, OSPF computes the link cost of each interface from the interface bandwidth. Faster links have lower metrics, making them more attractive in route selection. The configuration parameters in the **auto-cost**, **reference-bandwidth**, and **bandwidth** commands give you control over the default link cost. You can configure for OSPF an interface bandwidth that is independent of the actual link speed. A second configuration parameter allows you to control the ratio of interface bandwidth to link cost. The link cost is computed as the ratio of a reference bandwidth to the interface bandwidth ($\text{ref\_bw} / \text{interface bandwidth}$), in which interface bandwidth is defined by the **bandwidth** command.

Because the default reference bandwidth is 100 Mbps, OSPF uses the same default link cost for all interfaces whose bandwidth is 100 Mbps or greater. Use the **auto-cost** command to change the reference bandwidth, specifying the reference bandwidth in megabits per second (Mbps). For the *mbps* parameter, the reference bandwidth range is 1–4294967 Mbps.

Default	100 Mbps
Format	<code>auto-cost reference-bandwidth mbps</code>
Mode	Router OSPF Config

no auto-cost reference-bandwidth (Router OSPF Config)

Use this command to set the reference bandwidth to the default value.

Format	no auto-cost reference-bandwidth
Mode	Router OSPF Config

capability opaque

M4350

Use this command to enable opaque capability functionality on the switch. The information contained in opaque LSAs can be used directly by OSPF or indirectly by an application that distributes information throughout the OSPF domain. The switch supports storing and flooding of opaque LSAs of different scopes. When you enter the **capability opaque** command, OSPF forwards opaque LSAs by default.

Default	enabled
Format	capability opaque
Mode	Router Config

no capability opaque

Use this command to disable opaque capability on the router.

Format	no capability opaque
Mode	Router Config

clear ip ospf

M4350

Use this command to disable and re-enable OSPF.

Format	clear ip ospf
Mode	Privileged EXEC

clear ip ospf configuration

M4350

Use this command to reset the OSPF configuration to factory defaults.

Format	clear ip ospf configuration
Mode	Privileged EXEC

clear ip ospf counters

M4350

Use this command to reset global and interface statistics.

Format	<code>clear ip ospf counters</code>

Mode	Privileged EXEC

clear ip ospf neighbor

M4350

Use this command to drop the adjacency with all OSPF neighbors. On each neighbor's interface, send a one-way hello. Adjacencies may then be re-established. To drop all adjacencies with a specific router ID, specify the neighbor's router ID using the optional parameter *neighbor-id*.

Format	<code>clear ip ospf neighbor [<i>neighbor-id</i>]</code>

Mode	Privileged EXEC

clear ip ospf neighbor interface

M4350

To drop adjacency with all neighbors on a specific interface, use the optional parameter *unit/slot/port*. To drop adjacency with a specific router ID or IP address on a specific interface, use the optional parameter *neighbor-id*.

Format	<code>clear ip ospf neighbor interface [<i>unit/slot/port</i> <i>vlan vlan-id</i>] [<i>neighbor-id</i>]</code>

Mode	Privileged EXEC

clear ip ospf redistribution

M4350

Use this command to flush all self-originated external LSAs. Reapply the redistribution configuration and reoriginate prefixes as necessary.

Format	<code>clear ip ospf redistribution</code>

Mode	Privileged EXEC

default-information originate (Router OSPF Config)

M4350

This command is used to control the advertisement of default routes. The *metric* argument can be a number in the range 0–16777214. The metric type can be 1 or 2.

Default	metric—unspecified type—2
Format	default-information originate [always] [metric <i>metric</i>] [metric-type {1 2}]
Mode	Router OSPF Config

no default-information originate (Router OSPF Config)

This command is used to reset the advertisement of default routes to default values.

Format	no default-information originate [metric] [metric-type]
Mode	Router OSPF Config

default-metric (Router OSPF Config)

M4350

This command is used to set a default for the metric of distributed routes. The *metric* argument can be a number in the range 0–16777214.

Format	default-metric <i>metric</i>
Mode	Router OSPF Config

no default-metric (Router OSPF Config)

This command is used to reset the default for the metric of distributed routes.

Format	no default-metric
Mode	Router OSPF Config

distance ospf (Router OSPF Config)

M4350

This command sets the route preference value of OSPF on the switch. Lower route preference values are preferred when determining the best route. The type of OSPF route can be **intra-area**, **inter-area**, or **external**. All the external type routes are given the same preference value. The range of *preference* value is 1 to 255.

Default	110
Format	<code>distance ospf {intra-area <i>preference</i> inter-area <i>preference</i> external <i>preference</i>}</code>
Mode	Router OSPF Config

no distance ospf (Router OSPF Config)

This command resets the default route preference value of OSPF routes on the switch. The type of OSPF route can be **intra-area**, **inter-area**, or **external**.

Format	<code>no distance ospf {intra-area inter-area external}</code>
Mode	Router OSPF Config

distribute-list out (Router OSPF Config)

M4350

Use this command to specify the access list to filter routes received from the source protocol. The *access-list* argument can be a number from 1–199.

Format	<code>distribute-list <i>access-list</i> out {rip static connected}</code>
Mode	Router OSPF Config

no distribute-list out (Router OSPF Config)

Use this command to reset the access list to filter routes received from the source protocol.

Format	<code>no distribute-list <i>access-list</i> out {rip static connected}</code>
Mode	Router OSPF Config

distribute-list route-map (Router OSPF Config)

M4350

This command uses a route map to prevent the incoming OSPF routes from being added to the routing table. The route maps can match on one or more attributes of the OSPF route. The *name* argument is the name of an existing route map.

Format	<code>distribute-list route-map <i>name</i> in</code>
Mode	Router OSPF Config

no distribute-list route-map (Router OSPF Config)

Use this command to remove the route map for filtering incoming OSP routes.

Format	no distribute-list route-map in

Mode	Router OSPF Config

exit-overflow-interval (Router OSPF Config)

M4350

This command configures the exit overflow interval for OSPF. It describes the number of seconds after entering the overflow state that the switch waits before leaving the overflow state. This allows the switch to originate nondefault AS-external-LSAs again. When set to 0, the switch does not leave the overflow state until it is restarted. The range for the *seconds* argument is 0 to 2147483647 seconds.

Default	0

Format	exit-overflow-interval <i>seconds</i>

Mode	Router OSPF Config

no exit-overflow-interval (Router OSPF Config)

This command configures the default exit overflow interval for OSPF.

Format	no exit-overflow-interval

Mode	Router OSPF Config

external-lsdb-limit (Router OSPF Config)

M4350

This command configures the external LSDB limit for OSPF. If the value is -1, there is no limit. When the number of nondefault AS-external-LSAs in the switch's link-state database reaches the external LSDB limit, the switch enters the overflow state. The switch cannot hold more than the limit of external LSDB, nondefault AS-external-LSAs in its database. The external LSDB limit must be set identically in all routers (or routing-capable switches) attached to the OSPF backbone or any regular OSPF area. The range for the *limit* argument is -1 to 2147483647.

Default	-1

Format	external-lsdb-limit <i>limit</i>

Mode	Router OSPF Config

no external-lsdb-limit (Router OSPF Config)

This command configures the default external LSDB limit for OSPF.

Format	no external-lsdb-limit

Mode	Router OSPF Config

log-adjacency-changes

M4350

This command enables logging of OSPFv2 neighbor state changes. State changes are logged with the informational severity.

Default	Adjacency state changes are logged, but without the detail option.

Format	log-adjacency-changes [detail]

Mode	Router OSPF Config

Parameter	Description
detail	(Optional) When this keyword is specified, all adjacency state changes are logged. Otherwise, OSPF only logs transitions to FULL state and when a backwards transition occurs.

no log-adjacency-changes (Router OSPF Config)

This command disables the logging of OSPFv2 neighbor state changes.

Format	no log-adjacency-changes [detail]

Mode	Router OSPF Config

prefix-suppression (Router OSPF Config)

M4350

This command suppresses the advertisement of all the IPv4 prefixes except for prefixes that are associated with secondary IPv4 addresses, loopbacks, and passive interfaces from the OSPFv2 router advertisements.

To suppress a loopback or passive interface, use the `ip ospf prefix-suppression` command in interface configuration mode. Prefixes associated with secondary IPv4 addresses can never be suppressed.

Default	Prefix suppression is disabled.

Format	prefix-suppression

Mode	Router OSPF Config

no prefix-suppression (Router OSPF Config)

This command disables prefix-suppression. No prefixes are suppressed from getting advertised.

Format	no prefix-suppression

Mode	Router OSPF Config

router-id (Router OSPF Config)

M4350

This command sets a 4-digit dotted-decimal number uniquely identifying the router OSPF ID. The *ipaddress* is a configured value.

Format	router-id <i>ipaddress</i>

Mode	Router OSPF Config

no router-id (Router OSPF Config)

This command resets the router OSPF ID.

Format	no router-id

Mode	Router OSPF Config

redistribute (Router OSPF Config)

M4350

This command configures the OSPF protocol to allow redistribution of static, connected, or RIP routes. The *metric* argument is from 0 to 16777214. The **metric type** keyword can be 1 or 2. The *tag* argument is from 0 to 4294967295.

In addition, for the *route-map-name* argument, you can specify the name of an existing router map. You can also specify the **subnets** keyword to allow subnets to be redistributed into OSPF.

Default	metric: Not specified type: 2 tag: 0

Format	redistribute {static connected rip} [route-map <i>route-map-name</i> [metric <i>metric</i>] [metric-type {1 2}] [tag <i>tag</i>] [route-map <i>route-map-name</i>]] [subnets]

Mode	Router OSPF Config

Command example:

```
(NETGEAR Switch) (Config) #router ospf
(NETGEAR Switch) (config-router) #redistribute connected metric-type 1 route-map
SecureRoutes subnets
```

no redistribute (Router OSPF Config)

This command disables the OSPF protocol from redistributing static, connected, or RIP routes

Format	<code>no redistribute {static connected rip} [route-map [metric] [metric-type] [tag] [route-map]] [subnets]</code>

Mode	Router OSPF Config

maximum-paths (Router OSPF Config)**M4350**

This command sets the number of paths (from 1 to 16) that OSPF can report for a destination in which *maxpaths* is platform dependent.

Default	4

Format	<code>maximum-paths maxpaths</code>

Mode	Router OSPF Config

no maximum-paths (Router OSPF Config)

This command resets the number of paths that OSPF can report for a destination back to its default value.

Format	<code>no maximum-paths</code>

Mode	Router OSPF Config

passive-interface default (Router OSPF Config)**M4350**

Use this command to enable global passive mode by default for all interfaces. It overrides any interface level passive mode. OSPF will not form adjacencies over a passive interface.

Default	disabled

Format	<code>passive-interface default</code>

Mode	Router OSPF Config

no passive-interface default (Router OSPF Config)

Use this command to disable the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to nonpassive mode.

Format	no passive-interface default
Mode	Router OSPF Config

passive-interface (Router OSPF Config)

M4350

Use this command to set the interface as passive. It overrides the global passive mode that is currently effective on the interface. The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* can be a number from 1–4093.

Default	disabled
Format	passive-interface { <i>unit/slot/port</i> vlan <i>vlan-id</i> }
Mode	Router OSPF Config

no passive-interface (Router OSPF Config)

Use this command to set the interface as nonpassive. It overrides the global passive mode that is currently effective on the interface. The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* can be a number from 1–4093.

Format	no passive-interface { <i>unit/slot/port</i> vlan <i>vlan-id</i> }
Mode	Router OSPF Config

timers pacing flood (Router OSPF Config)

M4350

To adjust the rate at which OSPFv2 sends LS Update packets, use the `timers pacing flood` command in router OSPFv2 global configuration mode. OSPF distributes routing information in Link State Advertisements (LSAs), which are bundled into a Link State Update (LS Update) packets. To reduce the likelihood of sending a neighbor more packets than it can buffer, OSPF rate limits the transmission of LS Update packets. By default, OSPF sends up to 30 updates per second on each interface (1/the pacing interval). Use this command to adjust this packet rate.

Default	33 milliseconds
Format	<code>timers pacing flood milliseconds</code>
Mode	Router OSPF Config
Parameter	Description
milliseconds	The average time between transmission of LS Update packets. The range is from 5 ms to 100 ms. The default is 33 ms.

`no timers pacing flood` (Router OSPF Config)

This command reverts the LS Update packet rate to the default rate.

Format	<code>no timers pacing flood</code>
Mode	Router OSPF Config

`timers pacing lsa-group` (Router OSPF Config)

M4350

To adjust how OSPF groups refresh self-originated LSAs periodically, use the **`timers pacing lsa-group`** command in Router OSPF Config mode. OSPF refreshes self-originated LSAs approximately once every 30 minutes. When OSPF refreshes LSAs, it considers all self-originated LSAs whose age is from 1800 to 1800 plus the pacing group size. Grouping LSAs for refresh allows OSPF to combine refreshed LSAs into a minimal number of LS Update packets. Minimizing the number of Update packets makes LSA distribution more efficient.

When OSPF originates a new or changed LSA, it selects a random refresh delay for the LSA. When the refresh delay expires, OSPF refreshes the LSA. By selecting a random refresh delay, OSPF avoids refreshing a large number of LSAs at one time, even if a large number of LSAs are originated at one time.

Default	60 seconds
Format	<code>timers pacing lsa-group seconds</code>
Mode	Router OSPF Config
Parameter	Description
seconds	Width of the window in which LSAs are refreshed. The range for the pacing group window is from 10 to 1800 seconds.

no timers pacing lsa-group (Router OSPF Config)

This command reverts the period at which self-originated LSAs are refreshed to the default period.

Format	no timers pacing lsa-group
Mode	Router OSPF Config

timers spf (Router OSPF Config)

M4350

Use this command to configure the SPF delay time and hold time. The valid range for both the *delay time* and *hold time* parameters is from 1 to 600000 seconds.

Default	delay-time—5 hold-time—10
Format	timers spf delay-time hold-time
Mode	Router OSPF Config

no timers spf (Router OSPF Config)

This command reverts the SPF delay time and hold time to their default values.

Format	no timers spf
Mode	Router OSPF Config

trapflags (Router OSPF Config)

M4350

Use this command to enable individual OSPF traps, enable a group of trap flags at a time, or enable all the trap flags at a time. The different groups of trapflags, and each group's specific trapflags to enable or disable, are listed in the following table.

Table 10. Trapflags groups

Group	Flags
errors	- authentication-failure - bad-packet - config-error - virt-authentication-failure - virt-bad-packet - virt-config-error
lsa	- lsa-maxage - lsa-originate

Table 10. Trapflags groups

Group	Flags
overflow	- lsdb-overflow - lsdb-approaching-overflow
retransmit	- packets - virt-packets
state-change	- if-state-change - neighbor-state-change - virtif-state-change - virtneighbor-state-change

- To enable the individual flag, enter **trapflags** and the trapflag group name followed by the individual flag.
- To enable all the flags in that group, enter **trapflags** and the trapflag group name followed by **all**.
- To enable all flags, enter the command as **trapflags all**.

Default	disabled
Format	<pre>trapflags {all errors {all authentication-failure bad-packet config-error virt-authentication-failure virt-bad-packet virt-config-error} lsa {all lsa-maxage lsa-originate} overflow {all lsdb-overflow lsdb-approaching-overflow} retransmit {all packets virt-packets} state-change {all if-state-change neighbor-state-change virtif-state-change virtneighbor-state-change}}</pre>
Mode	Router OSPF Config

no trapflags (Router OSPF Config)

Use this command to revert to the default reference bandwidth.

- To disable the individual flag, enter **no trapflags** and the trapflag group name followed by the individual flag.
- To disable all the flags in that group, enter **no trapflags** and the trapflag group name followed by **all**.
- To disable all flags, enter the command as **no trapflags all**.

Format	<pre>no trapflags {all errors {all authentication-failure bad-packet config-error virt-authentication-failure virt-bad-packet virt-config-error} lsa {all lsa-maxage lsa-originate} overflow {all lsdb-overflow lsdb-approaching-overflow} retransmit {all packets virt-packets} state-change {all if-state-change neighbor-state-change virtif-state-change virtneighbor-state-change}}</pre>
Mode	Router OSPF Config

OSPF Interface Commands

Note: Open Shortest Path First (OSPF) commands are supported on the M4350 series switches only. The M4250 series switches do not support OSPF.

ip ospf area

M4350

Use this command to enable OSPFv2 and set the area ID of an interface or range of interfaces. The *area-id* is an IP address formatted as a 4-digit dotted-decimal number or a decimal value in the range of 0–4294967295. This command supersedes the effects of the **network area** command. It can also be used to configure the advertiseability of the secondary addresses on this interface into the OSPFv2 domain.

Default	disabled
Format	ip ospf area <i>area-id</i> [secondaries none]
Mode	Interface Config

no ip ospf area

Use this command to disable OSPF on an interface.

Format	no ip ospf area [secondaries none]
Mode	Interface Config

bandwidth

M4350

By default, OSPF computes the link cost of an interface as the ratio of the reference bandwidth to the interface bandwidth. Reference bandwidth is specified with the **auto-cost** command. For the purpose of the OSPF link cost calculation, use the bandwidth command to specify the interface bandwidth. The bandwidth is specified in kilobits per second; The *kbps* argument can be in the range 1–10000000. If no bandwidth is configured, the bandwidth defaults to the actual interface bandwidth for port-based routing interfaces and to 10 Mbps for VLAN routing interfaces. This command does not affect the actual speed of an interface. You can use this command to configure a single interface or a range of interfaces.

Default	actual interface bandwidth
Format	bandwidth <i>kbps</i>
Mode	Interface Config

no bandwidth

Use this command to set the interface bandwidth to its default value.

Format	no bandwidth

Mode	Interface Config

ip ospf authentication

M4350

This command sets the OSPF authentication type and key for the specified interface or range of interfaces. The type of authentication can be either **none**, **simple**, or **encrypt**. If you select **simple** or **encrypt**, the *key* parameter is composed of standard displayable, noncontrol keystrokes from a standard 101/102-key keyboard. The authentication *key* must be 8 bytes or less if the authentication type is **simple**. If the type is **encrypt**, the *key* can be up to 16 bytes. Unauthenticated interfaces do not need an authentication key. If the type is **encrypt**, a *keyid* in the range of 0 and 255 must be specified. The default value for authentication type is **none**. Neither the default password key nor the default key id are configured.

Format	ip ospf authentication {none simple key encrypt key keyid}

Mode	Interface Config

no ip ospf authentication

This command resets the default OSPF authentication type for the interface.

Format	no ip ospf authentication

Mode	Interface Config

ip ospf cost

M4350

This command configures the cost on an OSPF interface or range of interfaces. The *cost* parameter has a range of 1 to 65535.

Default	10

Format	ip ospf cost cost

Mode	Interface Config

no ip ospf cost

This command configures the default cost on an OSPF interface.

Format	no ip ospf cost
Mode	Interface Config

ip ospf database-filter all out

M4350

This command disables OSPFv2 LSA flooding on an interface. Use this command in Interface Configuration mode.

Default	Disabled
Format	ip ospf database-filter all out
Mode	Interface Configuration

no ip ospf database-filter all out

This command enables OSPFv2 LSA flooding on an interface. Use this command in Interface Configuration mode.

Default	Disabled
Format	no ip ospf database-filter all out
Mode	Interface Configuration

ip ospf dead-interval

M4350

This command sets the OSPF dead interval for the specified interface or range of interfaces. The value for *seconds* is a valid positive integer in the range 1–65535 and represents the period in seconds that a router's Hello packets are allowed to go undetected before its neighbor routers declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (for example, 4).

Default	40
Format	ip ospf dead-interval <i>seconds</i>
Mode	Interface Config

no ip ospf dead-interval

This command sets the default OSPF dead interval for the specified interface.

Format	no ip ospf dead-interval

Mode	Interface Config

ip ospf hello-interval

M4350

This command sets the OSPF hello interval for the specified interface or range of interfaces. The value for seconds is a valid positive integer, which represents the length of time in seconds. The value for the period must be the same for all routers attached to a network. Valid values for *seconds* are in the range from 1 to 65535.

Default	10

Format	ip ospf hello-interval <i>seconds</i>

Mode	Interface Config

no ip ospf hello-interval

This command sets the default OSPF hello interval for the specified interface.

Format	no ip ospf hello-interval

Mode	Interface Config

ip ospf network

M4350

Use this command to configure OSPF to treat an interface or range of interfaces as a point-to-point rather than broadcast interface. The **broadcast** option sets the OSPF network type to broadcast. The **point-to-point** option sets the OSPF network type to point-to-point. OSPF treats interfaces as broadcast interfaces by default. (Loopback interfaces have a special loopback network type, which cannot be changed.) When there are only two routers on the network, OSPF can operate more efficiently by treating the network as a point-to-point network. For point-to-point networks, OSPF does not elect a designated router or generate a network link state advertisement (LSA). Both endpoints of the link must be configured to operate in point-to-point mode.

Default	broadcast

Format	ip ospf network {broadcast point-to-point}

Mode	Interface Config

no ip ospf network

Use this command to return the OSPF network type to the default.

Format	no ip ospf network
Mode	Interface Config

ip ospf prefix-suppression

M4350

This command suppresses the advertisement of the IPv4 prefixes that are associated with an interface, except for those associated with secondary IPv4 addresses. This command takes precedence over the global configuration. If this configuration is not specified, the global prefix-suppression configuration applies.

prefix-suppression can be disabled at the interface level by using the disable option. The disable option is useful for excluding specific interfaces from performing prefix-suppression when the feature is enabled globally.

Note that the disable option disable is not equivalent to not configuring the interface specific prefix-suppression. If prefix-suppression is not configured at the interface level, the global prefix-suppression configuration is applicable for the IPv4 prefixes associated with the interface.

Default	Prefix-suppression is not configured.
Format	ip ospf prefix-suppression [disable]
Mode	Interface Config

no ip ospf prefix-suppression

This command removes prefix-suppression configurations at the interface level. When you enter the **no ip ospf prefix-suppression** command, global prefix-suppression applies to the interface. Not configuring the command is not equal to disabling interface level prefix-suppression.

Format	no ip ospf prefix-suppression
Mode	Interface Config

ip ospf priority

M4350

This command sets the OSPF priority for the specified router interface or range of interfaces. The *priority* argument for the interface is a priority integer from 1 to 255, in which 1 is the

lowest priority and 255 is the highest priority. A value of 0 indicates that the switch is not eligible to become the designated router on this network.

Default	1
Format	<code>ip ospf priority <i>priority</i></code>
Mode	Interface Config

no ip ospf priority

This command sets the default OSPF priority for the specified router interface.

Format	<code>no ip ospf priority</code>
Mode	Interface Config

ip ospf retransmit-interval

M4350

This command sets the OSPF retransmit Interval for the specified interface or range of interfaces. The retransmit interval is specified in seconds. The value for *seconds* is the number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. The value for *second* ranges from 0 to 3600 (1 hour).

Default	5
Format	<code>ip ospf retransmit-interval <i>second</i></code>
Mode	Interface Config

no ip ospf retransmit-interval

This command sets the default OSPF retransmit Interval for the specified interface.

Format	<code>no ip ospf retransmit-interval</code>
Mode	Interface Config

ip ospf transmit-delay

M4350

This command sets the OSPF Transit Delay for the specified interface or range of interfaces. The transmit delay is specified in seconds. In addition, it sets the estimated number of seconds it takes to transmit a link state update packet over this interface. The value for *second* ranges from 0 to 3600 (1 hour).

Default	1
Format	<code>ip ospf transmit-delay <i>second</i></code>
Mode	Interface Config

`no ip ospf transmit-delay`

This command sets the default OSPF Transit Delay for the specified interface.

Format	<code>no ip ospf transmit-delay</code>
Mode	Interface Config

`ip ospf mtu-ignore`

M4350

This command disables OSPF maximum transmission unit (MTU) mismatch detection on an interface or range of interfaces. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When the switch receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the switch can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

Default	enabled
Format	<code>ip ospf mtu-ignore</code>
Mode	Interface Config

`no ip ospf mtu-ignore`

This command enables the OSPF MTU mismatch detection.

Format	<code>no ip ospf mtu-ignore</code>
Mode	Interface Config

OSPF Graceful Restart Commands

Note: Open Shortest Path First (OSPF) commands are supported on the M4350 series switches only. The M4250 series switches do not support OSPF.

The OSPF protocol can be configured to participate in the checkpointing service, so that these protocols can execute a graceful restart” when the management unit fails. In a graceful restart, the hardware to continues forwarding IPv4 packets using OSPF routes while a backup switch takes over management unit responsibility

Graceful restart uses the concept of helpful neighbors. A fully adjacent router enters helper mode when it receives a link state announcement (LSA) from the restarting management unit indicating its intention of performing a graceful restart. In helper mode, a switch continues to advertise to the rest of the network that they have full adjacencies with the restarting router, thereby avoiding announcement of a topology change and the potential for flooding of LSAs and shortest-path-first (SPF) runs (which determine OSPF routes). Helpful neighbors continue to forward packets through the restarting router. The restarting router relearns the network topology from its helpful neighbors.

Graceful restart can be enabled for either planned or unplanned restarts, or both. A planned restart is initiated by the operator through the **initiate failover** command. The operator may initiate a failover in order to take the management unit out of service (for example, to address a partial hardware failure), to correct faulty system behavior which cannot be corrected through less severe management actions, or other reasons. An unplanned restart is an unexpected failover caused by a fatal hardware failure of the management unit or a software hang or crash on the management unit.

nsf (Router OSPF Config)

M4350

Use this command to enable the OSPF graceful restart functionality on an interface.

Default	Disabled
Format	nsf [ietf] [planned-only]
Modes	Router OSPF Config

Parameter	Description
ietf	This keyword is accepted but not required.
planned-only	This optional keyword indicates that OSPF should only perform a graceful restart when the restart is planned (that is, when the restart is a result of the initiate failover command).

no nsf (Router OSPF Config)

Use this command to disable graceful restart.

Format	no [ietf] nsf
Modes	Router OSPF Config

nsf restart-interval (Router OSPF Config)

M4350

Use this command to configure the number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. This is referred to as the grace period. The restarting router includes the grace period in its grace LSAs. For planned restarts (using the **initiate failover** command), the grace LSAs are sent prior to restarting the management unit, whereas for unplanned restarts, they are sent after reboot begins.

The grace period must be set long enough to allow the restarting router to reestablish all of its adjacencies and complete a full database exchange with each of those neighbors. The value for the *seconds* argument can be from 1–1800 seconds.

Default	120 seconds
Format	nsf [ietf] restart-interval <i>seconds</i>
Modes	Router OSPF Config

Parameter	Description
ietf	This keyword is accepted but not required.
seconds	The number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. The range is from 1 to 1800 seconds.

no nsf restart-interval (Router OSPF Config)

Use this command to revert the grace period to its default value.

Format	no [ietf] nsf restart-interval
Modes	Router OSPF Config

nsf helper (Router OSPF Config)

M4350

Use this command to enable helpful neighbor functionality for the OSPF protocol. You can enable this functionality for planned or unplanned restarts, or both.

Default	OSPF may act as a helpful neighbor for both planned and unplanned restarts
Format	<code>nsf helper [planned-only]</code>
Modes	Router OSPF Config
Parameter	Description
planned-only	This optional keyword indicates that OSPF should only help a restarting router performing a planned restart.

no nsf helper (Router OSPF Config)

Use this command to disable helpful neighbor functionality for OSPF.

Format	<code>no nsf helper</code>
Modes	Router OSPF Config

nsf ietf helper disable (Router OSPF Config)

M4350

Use this command to disable helpful neighbor functionality for OSPF.

Note: The commands `no nsf helper` and `nsf ietf helper disable` are functionally equivalent. The command `nsf ietf helper disable` is supported solely for compatibility with other network software CLI.

Format	<code>nsf ietf helper disable</code>
Modes	Router OSPF Config

nsf helper strict-lsa-checking (Router OSPF Config)

M4350

The restarting router is unable to react to topology changes. In particular, the restarting router does not immediately update its forwarding table; therefore, a topology change may introduce forwarding loops or black holes that persist until the graceful restart completes. By exiting the graceful restart on a topology change, a router tries to eliminate the loops or black holes as quickly as possible by routing around the restarting router. A helpful neighbor

considers a link down with the restarting router to be a topology change, regardless of the strict LSA checking configuration.

Use this command to require that an OSPF helpful neighbor exit helper mode whenever a topology change occurs.

Default	Enabled.
Format	<code>nsf [ietf] helper strict-lsa-checking</code>
Modes	Router OSPF Config

Parameter	Description
ietf	This keyword is accepted but not required.

`no nsf helper strict-lsa-checking` (Router OSPF Config)

Use this command to allow OSPF to continue as a helpful neighbor in spite of topology changes.

Default	Enabled.
Format	<code>nsf [ietf] helper strict-lsa-checking</code>
Modes	Router OSPF Config

OSPFv2 Stub Router Commands

Note: Open Shortest Path First (OSPF) commands are supported on the M4350 series switches only. The M4250 series switches do not support OSPF.

`max-metric router-lsa` (Router OSPF Config)

M4350

To configure OSPF to enter stub router mode, use this command in Router OSPF Configuration mode. When OSPF is in stub router mode, as defined by RFC 3137, OSPF sets the metric in the nonstub links in its router LSA to `LsInfinity`. Other routers therefore compute very long paths through the stub router, and prefer any alternate path. Doing so eliminates all transit traffic through the stub router, when alternate routes are available. Stub router mode is useful when adding or removing a router from a network or to avoid transient routes when a router reloads.

You can administratively force OSPF into stub router mode. OSPF remains in stub router mode until you take OSPF out of stub router mode. Alternatively, you can configure OSPF to start in stub router mode for a configurable period of time after the router boots up.

If you set the summary LSA metric to 16,777,215, other routers will skip the summary LSA when they compute routes.

If you have configured the router to enter stub router mode on startup and then enter the **max-metric router lsa** command, there is no change. If OSPF is administratively in stub router mode (that is, you entered the **max-metric router-lsa** command), and you configure OSPF to enter stub router mode on startup (that is, the switch enters the **max-metric router-lsa** command on startup), OSPF exits stub router mode (assuming that the startup period has expired) and the configuration is updated.

Default	OSPF is not in stub router mode by default
Format	<code>max-metric router-lsa [on-startup seconds] [summary-lsa metric]</code>
Mode	Router OSPF Config

Parameter	Description
on-startup	(Optional) OSPF starts in stub router mode after a reboot.
seconds	(Required if on-startup) The number of seconds that OSPF remains in stub router mode after a reboot. The range is 5 to 86,400 seconds. There is no default value.
summary-lsa	(Optional) Set the metric in type 3 and type 4 summary LSAs to LsInfinity (0xFFFFFFFF).
metric	(Optional) Metric to send in summary LSAs when in stub router mode. The range is 1 to 16,777,215. The default is 16,711,680 (0xFF0000).

`no max-metric router-lsa`

Use this command in Router OSPF Config mode to disable stub router mode. The command clears either type of stub router mode (always or on-startup) and resets the **summary-lsa** option. If OSPF is configured to enter global configuration mode on startup, and during normal operation you want to immediately place OSPF in stub router mode, issue the **no max-metric router-lsa on-startup** command. The **no max-metric router-lsa summary-lsa** command causes OSPF to send summary LSAs with metrics computed using normal procedures defined in RFC 2328.

Format	<code>no max-metric router-lsa [on-startup] [summary-lsa]</code>
Mode	Router OSPF Config

`clear ip ospf stub-router`

M4350

This command forces OSPF to exit stub router mode when it has automatically entered stub router mode because of a resource limitation. OSPF only exits stub router mode if it entered stub router mode because of a resource limitation or if it is in stub router mode at startup. If OSPF is configured to function permanently in stub router mode, the command does not take effect.

Format	<code>clear ip ospf stub-router</code>

Mode	Privileged EXEC

OSPF Show Commands

Note: Open Shortest Path First (OSPF) commands are supported on the M4350 series switches only. The M4250 series switches do not support OSPF.

show ip ospf

M4350

This command displays information relevant to OSPF on the switch.

Format	<code>show ip ospf</code>

Mode	Privileged EXEC

Note: Some of the information below displays only if you enable OSPF and configure certain features.

Term	Definition
Router ID	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
OSPF Admin Mode	Shows whether the administrative mode of OSPF in the router is enabled or disabled. This is a configured value.
RFC 1583 Compatibility	Indicates whether 1583 compatibility is enabled or disabled. This is a configured value.
External LSDB Limit	The maximum number of nondefault AS-external-LSA (link state advertisement) entries that can be stored in the link-state database.
Exit Overflow Interval	The number of seconds that, after entering overflow state, a router will attempt to leave overflow state.
Spf Delay Time	The number of seconds between two subsequent changes of LSAs, during which time the routing table calculation is delayed.
Spf Hold Time	The number of seconds between two consecutive spf calculations.

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Flood Pacing Interval	The average time, in milliseconds, between LS Update packet transmissions on an interface. This is the value configured with the command <code>timers pacing flood</code> (Router OSPF Config) on page 1032.
LSA Refresh Group Pacing Time	The size in seconds of the LSA refresh group window. This is the value configured with the command <code>timers pacing lsa-group</code> (Router OSPF Config) on page 1033.
Opaque Capability	Shows whether the router is capable of sending Opaque LSAs. This is a configured value.
Autocost Ref BW	Shows the value of auto-cost reference bandwidth configured on the router.
Default Passive Setting	Shows whether the interfaces are passive by default.
Maximum Paths	The maximum number of paths that OSPF can report for a destination.
Default Metric	Default value for redistributed routes.
Stub Router Configuration	When OSPF runs out of resources to store the entire link state database, or any other state information, OSPF goes into stub router mode. As a stub router, OSPF reoriginates its own router LSAs, setting the cost of all nonstub interfaces to infinity. Use this field to set stub router configuration to one of Always, Startup, None.
Stub Router Startup Time	Configured value in seconds. This row is only listed if OSPF is configured to be a stub router at startup.
Summary LSA Metric Override	One of Enabled (met), Disabled, in which met is the metric to be sent in summary LSAs when in stub router mode.
Default Route Advertise	Indicates whether the default routes received from other source protocols are advertised or not.
Always	Shows whether default routes are always advertised.
Metric	The metric of the routes being redistributed. If the metric is not configured, this field is blank.
Metric Type	Shows whether the routes are External Type 1 or External Type 2.
Number of Active Areas	The number of active OSPF areas. An active OSPF area is an area with at least one interface up.
ABR Status	Shows whether the router is an OSPF Area Border Router.
ASBR Status	Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. The router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocols. The possible values for the ASBR status is enabled (if the router is configured to redistribute routes learned by other protocols) or disabled (if the router is not configured for the same).
Stub Router Status	One of Active, Inactive.
Stub Router Reason	One of Configured, Startup, Resource Limitation. Note: The row is only listed if stub router is active.
Stub Router Startup Time Remaining	The remaining time, in seconds, until OSPF exits stub router mode. This row is only listed if OSPF is in startup stub router mode.

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Stub Router Duration	The time elapsed since the router last entered the stub router mode. The row is only listed if stub router is active and the router entered stub mode because of a resource limitation. The duration is displayed in DD:HH:MM:SS format.
External LSDB Overflow	When the number of nondefault external LSAs exceeds the configured limit, External LSDB Limit, OSPF goes into LSDB overflow state. In this state, OSPF withdraws all of its self-originated nondefault external LSAs. After the Exit Overflow Interval, OSPF leaves the overflow state, if the number of external LSAs has been reduced.
External LSA Count	The number of external (LS type 5) link-state advertisements in the link-state database.
External LSA Checksum	The sum of the LS checksums of external link-state advertisements contained in the link-state database.
AS_OPAQUE LSA Count	Shows the number of AS Opaque LSAs in the link-state database.
AS_OPAQUE LSA Checksum	Shows the sum of the LS Checksums of AS Opaque LSAs contained in the link-state database.
New LSAs Originated	The number of new link-state advertisements that have been originated.
LSAs Received	The number of link-state advertisements received determined to be new instantiations.
LSA Count	The total number of link state advertisements currently in the link state database.
Maximum Number of LSAs	The maximum number of LSAs that OSPF can store.
LSA High Water Mark	The maximum size of the link state database since the system started.
AS Scope LSA Flood List Length	The number of LSAs currently in the global flood queue waiting to be flooded through the OSPF domain. LSAs with AS flooding scope, such as type 5 external LSAs and type 11 Opaque LSAs.
Retransmit List Entries	The total number of LSAs waiting to be acknowledged by all neighbors. An LSA may be pending acknowledgment from more than one neighbor.
Maximum Number of Retransmit Entries	The maximum number of LSAs that can be waiting for acknowledgment.
Retransmit Entries High Water Mark	The maximum number of LSAs on all neighbors' retransmit lists.
NSF Support	Indicates whether nonstop forwarding (NSF) is enabled for the OSPF protocol for planned restarts, unplanned restarts or both (Always).
NSF Restart Interval	The user-configurable grace period during which a neighboring router will be in the helper state after receiving notice that the management unit is performing a graceful restart.

Term	Definition
NSF Restart Status	The current graceful restart status of the router. • Not Restarting • Planned Restart • Unplanned Restart
NSF Restart Age	Number of seconds until the graceful restart grace period expires.
NSF Restart Exit Reason	Indicates why the router last exited the last restart: • None—Graceful restart has not been attempted. • In Progress—Restart is in progress. • Completed—The previous graceful restart completed successfully. • Timed Out—The previous graceful restart timed out. • Topology Changed—The previous graceful restart terminated prematurely because of a topology change.
NSF Help Support	Indicates whether helpful neighbor functionality has been enabled for OSPF for planned restarts, unplanned restarts, or both (Always).
NSF help Strict LSA checking	Indicates whether strict LSA checking has been enabled. If enabled, then an OSPF helpful neighbor will exit helper mode whenever a topology change occurs. If disabled, an OSPF neighbor will continue as a helpful neighbor in spite of topology changes.
Prefix-suppression	Displays whether prefix-suppression is enabled or disabled.

```
(alpha3) #show ip ospf
```

```

Router ID..... 3.3.3.3
OSPF Admin Mode..... Enable
RFC 1583 Compatibility..... Enable
External LSDB Limit..... No Limit
Exit Overflow Interval..... 0
Spf Delay Time..... 5
Spf Hold Time..... 10
Flood Pacing Interval..... 33 ms
LSA Refresh Group Pacing Time..... 60 sec
Opaque Capability..... Enable
AutoCost Ref BW..... 100 Mbps
Default Passive Setting..... Disabled
Maximum Paths..... 4
Default Metric..... Not configured
Stub Router Configuration..... <val>
Stub Router Startup Time..... <val> seconds
Summary LSA Metric Override..... Enabled (<met>)

Default Route Advertise..... Disabled
Always..... FALSE
Metric..... Not configured
Metric Type..... External Type 2

```

```

Number of Active Areas..... 1 (1 normal, 0 stub, 0 nssa)
ABR Status..... Disable
ASBR Status..... Disable
Stub Router..... FALSE
Stub Router Status..... Inactive
Stub Router Reason..... <reason>
Stub Router Startup Time Remaining..... <duration> seconds
Stub Router Duration..... <duration>
External LSDB Overflow..... FALSE
External LSA Count..... 0
External LSA Checksum..... 0
AS_OPAQUE LSA Count..... 0
AS_OPAQUE LSA Checksum..... 0
New LSAs Originated..... 55
LSAs Received..... 82
LSA Count..... 1
Maximum Number of LSAs..... 24200
LSA High Water Mark..... 9
AS Scope LSA Flood List Length..... 0
Retransmit List Entries..... 0
Maximum Number of Retransmit Entries..... 96800
Retransmit Entries High Water Mark..... 1
NSF Helper Support..... Always
NSF Helper Strict LSA Checking..... Enabled
Prefix-suppression..... Disabled

```

show ip ospf abr

M4350

This command displays the internal OSPF routing table entries to Area Border Routers (ABR).

Format	show ip ospf abr
Mode	Privileged EXEC User EXEC
Term	Definition
Type	The type of the route to the destination. It can be either: • intra — Intra-area route • inter — Inter-area route
Router ID	Router ID of the destination.

Term	Definition
Cost	Cost of using this route.
Area ID	The area ID of the area from which this route is learned.
Next Hop	Next hop toward the destination.
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

show ip ospf area

M4350

This command displays information about the area. The *area-id* identifies the OSPF area that is being displayed.

Format	<code>show ip ospf area area-id</code>
Modes	Privileged EXEC User EXEC

Term	Definition
AreaID	The area id of the requested OSPF area.
External Routing	A number representing the external routing capabilities for this area.
Spf Runs	The number of times that the intra-area route table has been calculated using this area's link-state database.
Area Border Router Count	The total number of area border routers reachable within this area.
Area LSA Count	Total number of link-state advertisements in this area's link-state database, excluding AS External LSA's.
Area LSA Checksum	A number representing the Area LSA Checksum for the specified AreaID excluding the external (LS type 5) link-state advertisements.
Flood List Length	The number of LSAs waiting to be flooded within the area.
Import Summary LSAs	Shows whether to import summary LSAs.
OSPF Stub Metric Value	The metric value of the stub area. This field displays only if the area is configured as a stub area.

The following OSPF NSSA specific information displays only if the area is configured as an NSSA.

Term	Definition
Import Summary LSAs	Shows whether to import summary LSAs into the NSSA.
Redistribute into NSSA	Shows whether to redistribute information into the NSSA.
Default Information Originate	Shows whether to advertise a default route into the NSSA.
Default Metric	The metric value for the default route advertised into the NSSA.
Default Metric Type	The metric type for the default route advertised into the NSSA.
Translator Role	The NSSA translator role of the ABR, which is always or candidate.
Translator Stability Interval	The amount of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.
Translator State	Shows whether the ABR translator state is disabled, always, or elected.

Command example:

```
(R1) #show ip ospf area 1
```

```
AreaID..... 0.0.0.1
External Routing..... Import External LSAs
Spf Runs..... 10
Area Border Router Count..... 0
Area LSA Count..... 3004
Area LSA Checksum..... 0x5e0abed
Flood List Length..... 0
Import Summary LSAs..... Enable
```

show ip ospf asbr

M4350

This command displays the internal OSPF routing table entries to Autonomous System Boundary Routers (ASBR).

Format	show ip ospf asbr
Mode	Privileged EXEC User EXEC

Term	Definition
Type	The type of the route to the destination. It can be one of the following values: • intra — Intra-area route • inter — Inter-area route
Router ID	Router ID of the destination.
Cost	Cost of using this route.
Area ID	The area ID of the area from which this route is learned.
Next Hop	Next hop toward the destination.
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

show ip ospf database

M4350

This command displays information about the link state database when OSPF is enabled. If you do not enter any parameters, the command displays the LSA headers for all areas. Use the optional *area-id* parameter to display database information about a specific area. Use the optional parameters to specify the type of link state advertisements to display.

Format	<code>show ip ospf [[area-id] database [{database-summary [{asbr-summary external network nssa-external opaque-area opaque-as opaque-link router summary}}] [lsid] [{adv-router [ipaddr] self-originate}}]]]</code>
Mode	Privileged EXEC User EXEC

Parameter	Description
asbr-summary	Displays the autonomous system boundary router (ASBR) summary LSAs.
external	Displays the external LSAs.
network	Displays the network LSAs.
nssa-external	DisplayS NSSA external LSAs.
opaque-area	Displays area opaque LSAs.
opaque-as	Displays AS opaque LSAs.
opaque-link	Displays link opaque LSAs.
router	Displays router LSAs.
summary	Displays the LSA database summary information.
lsid	Specifies the link state ID (LSID). The value of <i>lsid</i> can be an IP address or an integer in the range of 0-4294967295.

Parameter	Description
adv-router	Displays the LSAs that are restricted by the advertising router.
self-originate	Displays the LSAs in that are self originated.

If OSPF is enabled, for each link-type and area, the following information is displayed:

Term	Definition
Link Id	A number that uniquely identifies an LSA that a router originates from all other self originated LSAs of the same LS type.
Adv Router	The Advertising Router. Is a 32-bit dotted decimal number representing the LSDB interface.
Age	A number representing the age of the link state advertisement in seconds.
Sequence	A number that represents which LSA is more recent.
Checksum	The total number LSA checksum.
Options	This is an integer. It indicates that the LSA receives special handling during routing calculations.
Rtr Opt	Router Options are valid for router links only.

show ip ospf database database-summary

M4350

Use this command to display the number of each type of LSA in the database for each area and for the router. The command also displays the total number of LSAs in the database.

Format	show ip ospf database database-summary
Modes	Privileged EXEC User EXEC

Term	Definition
Router	Total number of router LSAs in the OSPF link state database.
Network	Total number of network LSAs in the OSPF link state database.
Summary Net	Total number of summary network LSAs in the database.
Summary ASBR	Number of summary ASBR LSAs in the database.
Type-7 Ext	Total number of Type-7 external LSAs in the database.
Self-Originated Type-7	Total number of self originated AS external LSAs in the OSPF link state database.
Opaque Link	Number of opaque link LSAs in the database.
Opaque Area	Number of opaque area LSAs in the database.

Term	Definition
Subtotal	Number of entries for the identified area.
Opaque AS	Number of opaque AS LSAs in the database.
Total	Number of entries for all areas.

show ip ospf interface

M4350

This command displays the information for the physical interface or virtual interface tables. The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* can be a number from 1–4093.

Format	<code>show ip ospf interface {unit/slot/port vlan vlan-id loopback loopback-id}</code>
Mode	Privileged EXEC User EXEC

Term	Definition
IP Address	The IP address for the specified interface.
Subnet Mask	A mask of the network and host portion of the IP address for the OSPF interface.
Secondary IP Address(es)	The secondary IP addresses if any are configured on the interface.
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	The OSPF Area ID for the specified interface.
OSPF Network Type	The type of network on this interface that the OSPF is running on.
Router Priority	A number representing the OSPF Priority for the specified interface.
Retransmit Interval	A number representing the OSPF Retransmit Interval for the specified interface.
Hello Interval	A number representing the OSPF Hello Interval for the specified interface.
Dead Interval	A number representing the OSPF Dead Interval for the specified interface.
LSA Ack Interval	A number representing the OSPF LSA Acknowledgment Interval for the specified interface.
Transmit Delay	A number representing the OSPF Transmit Delay Interval for the specified interface.
Authentication Type	The OSPF Authentication Type for the specified interface are: none, simple, and encrypt.
Metric Cost	The cost of the OSPF interface.
Passive Status	Shows whether the interface is passive or not.

Term	Definition
OSPF MTU-ignore	Indicates whether to ignore MTU mismatches in database descriptor packets sent from neighboring routers.
Flood Blocking	Indicates whether flood blocking is enabled on the interface.

The information below displays only if OSPF is enabled.

Term	Definition
OSPF Interface Type	Broadcast LANs, such as Ethernet and IEEE 802.5, take the value <i>broadcast</i> . The OSPF Interface Type will be 'broadcast'.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.
Designated Router	The router ID representing the designated router.
Backup Designated Router	The router ID representing the backup designated router.
Number of Link Events	The number of link events.
Local Link LSAs	The number of Link Local Opaque LSAs in the link-state database.
Local Link LSA Checksum	The sum of LS Checksums of Link Local Opaque LSAs in the link-state database.
Prefix-suppression	Displays whether prefix-suppression is enabled, disabled, or unconfigured on the interface.

Command example:

The following output displays when the OSPF Admin Mode is disabled:

```
(NETGEAR Switch) #show ip ospf interface 1/0/1
```

```
IP Address..... 0.0.0.0
Subnet Mask..... 0.0.0.0
Secondary IP Address(es).....
OSPF Admin Mode..... Disable
OSPF Area ID..... 0.0.0.0
OSPF Network Type..... Broadcast
Router Priority..... 1
Retransmit Interval..... 5
Hello Interval..... 10
Dead Interval..... 40
LSA Ack Interval..... 1
Transmit Delay..... 1
Authentication Type..... None
Metric Cost..... 1 (computed)
Passive Status..... Non-passive interface
OSPF Mtu-ignore..... Disable
Flood Blocking..... Disable
```


OSPF is not enabled on this interface.

show ip ospf interface brief

M4350

This command displays brief information for the physical interface or virtual interface tables.

Format	show ip ospf interface brief
Mode	Privileged EXEC User EXEC
Term	Definition
Interface	The interface number.
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	The OSPF Area Id for the specified interface.
Router Priority	A number representing the OSPF Priority for the specified interface.
Cost	The metric cost of the OSPF interface.
Hello Interval	A number representing the OSPF Hello Interval for the specified interface.
Dead Interval	A number representing the OSPF Dead Interval for the specified interface.
Retransmit Interval	A number representing the OSPF Retransmit Interval for the specified interface.
Interface Transmit Delay	A number representing the OSPF Transmit Delay for the specified interface.
LSA Ack Interval	A number representing the OSPF LSA Acknowledgment Interval for the specified interface.

show ip ospf interface stats

M4350

This command displays the statistics for a specific interface. The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* can be a number from 1–4093.

Format	show ip ospf interface stats {unit/slot/port vlan vlan-id}
Modes	Privileged EXEC User EXEC

Term	Definition
OSPF Area ID	The area id of this OSPF interface.
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.
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 associated with this OSPF interface.
OSPF Interface Events	The number of times the specified OSPF interface has changed its state, or an error has 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 has changed state, or an error has 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. Note: This field applies only to OSPFv2.
Virtual Link Not Found	The number of received OSPF packets discarded where the ingress interface is in a nonbackbone 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.
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. Note: This field applies only to OSPFv2.
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. Note: This field applies only to OSPFv2.

Term	Definition
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. Note: Does not apply to Hellos.
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 has been reached for the number of neighbors on an interface or on the system as a whole.

The following table lists the number of OSPF packets of each type sent and received on the interface.

Packet Type	Sent	Received
Hello	6960	6960
Database Description	3	3
LS Request	1	1
LS Update	141	42
LS Acknowledgment	40	135

show ip ospf lsa-group

M4350

This command displays the number of self-originated LSAs within each LSA group.

Format `show ip ospf lsa-group`

Modes Privileged EXEC
 User EXEC

Field	Description
Total self-originated LSAs	The number of LSAs the router is currently originating.
Average LSAs per group	The number of self-originated LSAs divided by the number of LSA groups. The number of LSA groups is the refresh interval (1800 seconds) divided by the pacing interval (configured with <code>timers pacing lsa-group</code>) plus two.
Pacing group limit	The maximum number of self-originated LSAs in one LSA group. If the number of LSAs in a group exceeds this limit, OSPF redistributes LSAs throughout the refresh interval to achieve better balance.
Groups	For each LSA pacing group, the output shows the range of LSA ages in the group and the number of LSAs in the group.

show ip ospf neighbor

M4350

This command displays information about OSPF neighbors. If you do not specify a neighbor IP address, the output displays summary information in a table. If you specify an interface, only the information for that interface displays.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* can be a number from 1–4093.

The *ip-address* argument is the IP address of the neighbor, and when you specify this, detailed information about the neighbor displays.

Format	show ip ospf neighbor [interface { <i>unit/slot/port</i> <i>vlan vlan-id</i> }] [<i>ip-address</i>]
Modes	Privileged EXEC User EXEC

If you do not specify an IP address, a table with the following columns displays for all neighbors or the neighbor associated with the interface that you specify:

Term	Definition
Router ID	The 4-digit dotted-decimal number of the neighbor 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.
IP Address	The IP address of the neighbor.
Interface	The interface of the local router in the <i>unit/slot/port</i> format.
State	The state of the neighboring routers. Possible values are: • Down. Initial state of the neighbor conversation; no recent information has been received from the neighbor. • Attempt. No recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor. • Init. An Hello packet has recently been seen from the neighbor, but bidirectional communication has not yet been established. • 2 way. Communication between the two routers is bidirectional. • Exchange start. The first step in creating an adjacency between the two neighboring routers, the goal being to decide which router is the primary router and what the initial DD sequence number is. • Exchange. The router is describing its entire link state database by sending Database Description packets to the neighbor. • Loading. Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state. • Full. The neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.

Term	Definition
Dead Time	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.

If you specify an IP address for the neighbor router, the following fields display.

Term	Definition
Interface	The interface number.
Neighbor IP Address	The IP address of the neighbor router.
Interface Index	The interface ID of the neighbor router.
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 (that is, neighbor relationships will 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.
Dead Timer Due	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.
Up Time	Neighbor uptime; how long since the adjacency last reached the Full state.
State	The state of the neighboring routers.
Events	The number of times this neighbor relationship has changed state, or an error has occurred.
Retransmitted LSAs	The number of LSAs retransmitted to this neighbor.
Retransmission Queue Length	An integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.
Restart Helper Status	Indicates the status of this router as a helper during a graceful restart of the router specified in the command line: • Helping. This router is acting as a helpful neighbor to this neighbor. A helpful neighbor does not report an adjacency change during graceful restart, but continues to advertise the restarting router as a FULL adjacency. A helpful neighbor continues to forward data packets to the restarting router, trusting that the restarting router's forwarding table is maintained during the restart. • Not Helping. This router is not a helpful neighbor at this time.

Term	Definition
Restart Reason	When this router is in helpful neighbor mode, this indicates the reason for the restart as provided by the restarting router: • Unknown (0) • Software restart (1) • Software reload/upgrade (2) • Switch to redundant control processor (3) • Unrecognized - a value not defined in RFC 3623 When the switch sends a grace LSA, it sets the Restart Reason to Software Restart on a planned warm restart (when the initiate failover command is invoked), and to Unknown on an unplanned warm restart.
Remaining Grace Time	The number of seconds remaining the in current graceful restart interval. This is displayed only when this router is currently acting as a helpful neighbor for the router specified in the command.
Restart Helper Exit Reason	Indicates the reason that the specified router last exited a graceful restart. • None. Graceful restart has not been attempted • In Progress. Restart is in progress • Completed. The previous graceful restart completed successfully • Timed Out. The previous graceful restart timed out • Topology Changed. The previous graceful restart terminated prematurely because of a topology change

Command example:

```
(alpha1) #show ip ospf neighbor 170.1.1.50

Interface.....0/17
Neighbor IP Address.....170.1.1.50
Interface Index.....17
Area Id.....0.0.0.2
Options.....0x2
Router Priority.....1
Dead timer due in (secs).....15
Up Time.....0 days 2 hrs 8 mins 46 secs
State.....Full/BACKUP-DR
Events.....4
Retransmitted LSAs.....32
Retransmission Queue Length.....0
Restart Helper Status..... Helping
Restart Reason..... Software Restart (1)
Remaining Grace Time..... 10 sec
Restart Helper Exit Reason..... In Progress
```

show ip ospf range

M4350

This command displays the set of OSPFv2 area ranges configured for a specified area.

Format	<code>show ip ospf range area-id</code>

Modes	Privileged EXEC

Term	Definition
Prefix	The summary prefix.
Subnet Mask	The subnetwork mask of the summary prefix.
Type	S (Summary Link) or E (External Link)
Action	Advertise or Suppress
Cost	Metric to be advertised when the range is active. If a static cost is not configured, the field displays Auto. If the action is Suppress, the field displays N/A.
Active	Whether the range is currently active. Y or N.

Command example:

```
(R1) #show ip ospf range 0
```

Prefix	Subnet Mask	Type	Action	Cost	Active
10.1.0.0	255.255.0.0	S	Advertise	Auto	N
172.20.0.0	255.255.0.0	S	Advertise	500	Y

show ip ospf statistics

M4350

This command displays information about recent Shortest Path First (SPF) calculations. The SPF is the OSPF routing table calculation. The output lists the number of times the SPF has run for each OSPF area. A table follows this information. For each of the 15 most recent SPF runs, the command shows statistics for how long ago the SPF ran, how long the SPF took, the reasons why the SPF was scheduled, the individual components of the routing table calculation time and to show the RIB update time. The most recent statistics are displayed at the end of the table.

Format	<code>show ip ospf statistics</code>

Modes	Privileged EXEC

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Delta T	The time since the routing table was computed. The time is in the format hours, minutes, and seconds (hh:mm:ss).
Intra	The time taken to compute intra-area routes, in milliseconds.
Summ	The time taken to compute inter-area routes, in milliseconds.
Ext	The time taken to compute external routes, in milliseconds.
SPF Total	The total time to compute routes, in milliseconds. The total may exceed the sum of the Intra, Summ, and Ext times.
RIB Update	The time from the completion of the routing table calculation until all changes have been made in the common routing table [the Routing Information Base (RIB)], in milliseconds.
Reason	The event or events that triggered the SPF. Reason codes are as follows: • R. New router LSA • N. New network LSA • SN. New network summary LSA • SA. New ASBR summary LSA • X. New external LSA

Command example:

```
(NETGEAR Switch) #show ip ospf statistics
```

```
Area 0.0.0.0: SPF algorithm executed 15 times
```

Delta T	Intra	Summ	Ext	SPF Total	RIB Update	Reason
00:05:33	0	0	0	0	0	R
00:05:30	0	0	0	0	0	R
00:05:19	0	0	0	0	0	N, SN
00:05:15	0	10	0	10	0	R, N, SN
00:05:11	0	0	0	0	0	R
00:04:50	0	60	0	60	460	R, N
00:04:46	0	90	0	100	60	R, N
00:03:42	0	70	10	90	160	R
00:03:39	0	70	40	120	240	X
00:03:36	0	60	60	130	160	X
00:01:28	0	60	50	130	240	X
00:01:25	0	30	50	110	310	SN
00:01:22	0	0	40	50	260	SN
00:01:19	0	0	20	20	190	X
00:01:16	0	0	0	0	110	R, X

show ip ospf stub table

M4350

This command displays the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

Format	show ip ospf stub table
Modes	Privileged EXEC User EXEC
Term	Definition
Area ID	A 32-bit identifier for the created stub area.
Type of Service	The type of service associated with the stub metric. NETGEAR supports only Normal TOS.
Metric Val	The metric value is applied based on the TOS. It defaults to the least metric of the type of service among the interfaces to other areas. The OSPF cost for a route is a function of the metric value.
Import Summary LSA	Controls the import of summary LSAs into stub areas.

show ip ospf traffic

M4350

This command displays OSPFv2 packet and LSA statistics and OSPFv2 message queue statistics. Packet statistics count packets and LSAs since OSPFv2 counters were last cleared (using the command [clear ip ospf counters](#) on page 1025).

Note: The [clear ip ospf counters](#) command does not clear the message queue high water marks.

Format	show ip ospf traffic
Modes	Privileged EXEC
Parameter	Description
OSPFv2 Packet Statistics	The number of packets of each type sent and received since OSPF counters were last cleared.
LSAs Retransmitted	The number of LSAs retransmitted by this router since OSPF counters were last cleared.
LS Update Max Receive Rate	The maximum rate of LS Update packets received during any 5-second interval since OSPF counters were last cleared. The rate is in packets per second.
LS Update Max Send Rate	The maximum rate of LS Update packets transmitted during any 5-second interval since OSPF counters were last cleared. The rate is in packets per second.

Parameter	Description
Number of LSAs Received	The number of LSAs of each type received since OSPF counters were last cleared.
OSPFv2 Queue Statistics	For each OSPFv2 message queue, the current count, the high water mark, the number of packets that failed to be enqueued, and the queue limit. The high water marks are not cleared when OSPF counters are cleared.

Command example:

```
(NETGEAR Switch) #show ip ospf traffic
```

```
Time Since Counters Cleared: 4000 seconds
```

OSPFv2 Packet Statistics

	Hello	Database Desc	LS Request	LS Update	LS ACK	Total
Recd:	500	10	20	50	20	600
Sent:	400	8	16	40	16	480

```
LSAs Retransmitted.....0
LS Update Max Receive Rate.....20 pps
LS Update Max Send Rate.....10 pps
```

Number of LSAs Received

```
T1 (NETGEAR Switch).....10
T2 (Network).....0
T3 (Net Summary).....300
T4 (ASBR Summary).....15
T5 (External).....20
T7 (NSSA External).....0
T9 (Link Opaque).....0
T10 (Area Opaque).....0
T11 (AS Opaque).....0
Total.....345
```

OSPFv2 Queue Statistics

	Current	Max	Drops	Limit
Hello	0	10	0	500
ACK	2	12	0	1680
Data	24	47	0	500
Event	1	8	0	1000

show ip ospf virtual-link

M4350

This command displays the OSPF Virtual Interface information for a specific area and neighbor. The *area-id* parameter identifies the area and the *neighbor* parameter identifies the neighbor's router ID.

Format	<code>show ip ospf virtual-link area-id neighbor</code>
Modes	Privileged EXEC User EXEC
Term	Definition
Area ID	The area id of the requested OSPF area.
Neighbor Router ID	The input neighbor Router ID.
Hello Interval	The configured hello interval for the OSPF virtual interface.
Dead Interval	The configured dead interval for the OSPF virtual interface.
Interface Transmit Delay	The configured transmit delay for the OSPF virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.
Authentication Type	The configured authentication type of the OSPF virtual interface.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPF interface.
Neighbor State	The neighbor state.

show ip ospf virtual-link brief

M4350

This command displays the OSPF Virtual Interface information for all areas in the system.

Format	<code>show ip ospf virtual-link brief</code>
Modes	Privileged EXEC User EXEC
Term	Definition
Area ID	The area id of the requested OSPF area.
Neighbor	The neighbor interface of the OSPF virtual interface.
Hello Interval	The configured hello interval for the OSPF virtual interface.
Dead Interval	The configured dead interval for the OSPF virtual interface.

Term	Definition
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.
Transmit Delay	The configured transmit delay for the OSPF virtual interface.

IP Event Dampening Commands

dampening

M4250

M4350

Use this command to enable IP event dampening on a routing interface.

Format	<code>dampening [half-life period] [reuse-threshold suppress-threshold max-suppress-time [restart restart-penalty]]</code>
Mode	Interface Config
Parameter	Description
Half-life period	The number of seconds it takes for the penalty to reduce by half. The configurable range is 1-30 seconds. Default value is 5 seconds.
Reuse Threshold	The value of the penalty at which the dampened interface is restored. The configurable range is 1-20,000. Default value is 1000.
Suppress Threshold	The value of the penalty at which the interface is dampened. The configurable range is 1-20,000. Default value is 2000.
Max Suppress Time	The maximum amount of time (in seconds) an interface can be in suppressed state after it stops flapping. The configurable range is 1-255 seconds. The default value is four times of half-life period. If half-period value is allowed to default, the maximum suppress time defaults to 20 seconds.
Restart Penalty	Penalty applied to the interface after the device reloads. The configurable range is 1-20,000. Default value is 2000.

no dampening

This command disables IP event dampening on a routing interface.

Format	<code>no dampening</code>
Mode	Interface Config

show dampening interface

M4250

M4350

This command summarizes the number of interfaces configured with dampening and the number of interfaces being suppressed.

Format	show dampening interface

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch)# show dampening interface
2 interfaces are configured with dampening.
1 interface is being suppressed.
```

show interface dampening

M4250

M4350

This command displays the status and configured parameters of the interfaces configured with dampening.

Format	show interface dampening

Mode	Privileged EXEC

Parameter	Description
Flaps	The number times the link state of an interface changed from UP to DOWN.
Penalty	Accumulated Penalty.
Supp	Indicates if the interface is suppressed or not.
ReuseTm	Number of seconds until the interface is allowed to come up again.
HalfL	Configured half-life period.
ReuseV	Configured reuse-threshold.
SuppV	Configured suppress threshold.
MaxSTm	Configured maximum suppress time in seconds.
MaxP	Maximum possible penalty.

Parameter	Description
Restart	Configured restart penalty.
Note: The command <code>clear counters on page 324</code> resets the flap count to zero.	
Note: Any change in the dampening configuration resets the current penalty, reuse time and suppressed state to their default values, meaning 0, 0, and <code>False</code> respectively.	

Command example:

```
Router# show interface dampening
```

```
Interface 0/2
```

Flaps	Penalty	Supp	ReuseTm	HalfL	ReuseV	SuppV	MaxSTm	MaxP	Restart
0	0	FALSE	0	5	1000	2000	20	16000	0

```
Interface 0/3
```

Flaps	Penalty	Supp	ReuseTm	HalfL	ReuseV	SuppV	MaxSTm	MaxP	Restart
6	1865	TRUE	18	20	1000	2001	30	2828	1500

Routing Information Protocol Commands

This section describes the commands you use to view and configure Routing Information Protocol (RIP), which is a distance-vector routing protocol that you use to route traffic within a small network.

router rip

M4250

M4350

Use this command to enter Router RIP Config mode.

Format	router rip

Mode	Global Config

enable (Router RIP Config)

M4250

M4350

This command sets the default administrative mode of RIP on the switch to active.

Default	enabled

Format	enable

Mode	Router RIP Config

no enable (Router RIP Config)

This command sets the administrative mode of RIP on the switch to inactive.

Format	no enable

Mode	Router RIP Config

ip rip

M4250

M4350

This command enables RIP on a router interface or range of interfaces.

Default	disabled

Format	ip rip

Mode	Interface Config

no ip rip

This command disables RIP on a router interface.

Format	no ip rip

Mode	Interface Config

auto-summary (Router RIP Config)

M4250

M4350

This command enables the RIP auto-summarization mode.

Default	disabled

Format	auto-summary

Mode	Router RIP Config

no auto-summary (Router RIP Config)

This command disables the RIP auto-summarization mode.

Format	no auto-summary

Mode	Router RIP Config

default-information originate (Router RIP Config)

M4250**M4350**

This command is used to control the advertisement of default routes.

Format	<code>default-information originate</code>
Mode	Router RIP Config

no default-information originate (Router RIP Config)

This command is used to control the advertisement of default routes.

Format	<code>no default-information originate</code>
Mode	Router RIP Config

default-metric (Router RIP Config)

M4250**M4350**

This command is used to set a default for the metric of distributed routes. The value for the *metric* argument can be from 0–15.

Format	<code>default-metric <i>metric</i></code>
Mode	Router RIP Config

no default-metric (Router RIP Config)

This command is used to reset the default metric of distributed routes to its default value.

Format	<code>no default-metric</code>
Mode	Router RIP Config

distance rip (Router RIP Config)

M4250**M4350**

This command sets the route preference value of RIP on the switch. Lower route preference values are preferred when determining the best route. A route with a preference of 255 cannot be used to forward traffic. The value for the *preference* argument can be from 1–255.

Default	15
Format	<code>distance rip preference</code>
Mode	Router RIP Config

no distance rip (Router RIP Config)

This command sets the default route preference value of RIP on the switch.

Format	<code>no distance rip</code>
Mode	Router RIP Config

distribute-list out (Router RIP Config)

M4250

M4350

This command is used to specify the access list to filter routes received from the source protocol. The value for the *access-list* argument can be from 1–199.

Default	0
Format	<code>distribute-list access-list out {static connected}</code>
Mode	Router RIP Config

no distribute-list out (Router RIP Config)

This command is used to specify the access list to filter routes received from the source protocol. The value for the *access-list* argument can be from 1–199.

Format	<code>no distribute-list access list out {static connected}</code>
Mode	Router RIP Config

ip rip authentication

M4250

M4350

This command sets the RIP version 2 authentication type and key for the interface or range of interfaces. The type of authentication can be either **none**, **simple**, or **encrypt**. If you select **simple** or **encrypt**, the *key* parameter is composed of standard displayable, noncontrol keystrokes from a standard 101/102-key keyboard. The authentication *key* must be 8 bytes or less if the authentication type is **simple**. If the type is **encrypt**, the *key* can be up to 16 bytes. Unauthenticated interfaces do not need an authentication key. If the type is **encrypt**, a *keyid* in the range of 0 and 255 must be specified. The default value for the

authentication type is **none**. Neither the default password key nor the default key id are configured.

Default	none
Format	<code>ip rip authentication {none {simple key} {encrypt key keyid}}</code>
Mode	Interface Config

no ip rip authentication

This command sets the default RIP Version 2 Authentication Type for an interface.

Format	<code>no ip rip authentication</code>
Mode	Interface Config

ip rip receive version

M4250

M4350

This command configures an interface or range of interfaces to allow RIP control packets of the specified version or versions to be received.

The options are: **rip1** to receive only RIP version 1 formatted packets; **rip2** for RIP version 2; **both** to receive packets from either format; or **none** to not allow any RIP control packets to be received.

Default	both
Format	<code>ip rip receive version {rip1 rip2 both none}</code>
Mode	Interface Config

no ip rip receive version

This command configures the interface to allow RIP control packets of the default version(s) to be received.

Format	<code>no ip rip receive version</code>
Mode	Interface Config

ip rip send version

M4250

M4350

This command configures an interface or range of interfaces to allow RIP control packets of the specified version to be sent.

The options are: **rip1** to send only RIP version-1 formatted packets; **rip2** for RIP version 2; **rip-1c** to send RIP version-2 formatted packets through a broadcast; or **none** to not allow any RIP control packets to be sent.

Default	rip2
Format	ip rip send version {rip1 rip1c rip2 none}
Mode	Interface Config

no ip rip send version

This command configures the interface to allow RIP control packets of the default version to be sent.

Format	no ip rip send version
Mode	Interface Config

hostroutesaccept (Router RIP Config)

M4250

M4350

This command enables the RIP hostroutesaccept mode.

Default	enabled
Format	hostroutesaccept
Mode	Router RIP Config

no hostroutesaccept (Router RIP Config)

This command disables the RIP hostroutesaccept mode.

Format	no hostroutesaccept
Mode	Router RIP Config

split-horizon (Router RIP Config)

M4250

M4350

This command sets the RIP split horizon mode. 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. The options are: **none**, no special processing; **simple**, a route is not included in updates sent to the router from which it was learned; **poison**, a route is included in updates sent to the router from which it was learned, but the metric is set to infinity.

Default	simple
Format	split-horizon {none simple poison}
Mode	Router RIP Config

no split-horizon (Router RIP Config)

This command sets the default RIP split horizon mode.

Format	no split-horizon
Mode	Router RIP Config

redistribute (Router RIP Config)

M4250

M4350

This command configures RIP protocol to redistribute static or connected routes. The *metric* argument is in the range from 0–15.

Default	0
Format	redistribute {static connected} [metric <i>metric</i>]
Mode	Router RIP Config

no redistribute (Router RIP Config)

This command disables RIP protocol to redistribute static or connected routes. The *metric* argument is in the range from 0–15.

Format	no redistribute {static connected} [metric <i>metric</i>]
Mode	Router RIP Config

redistribute ospf (Router RIP Config)

M4350

This command configures RIP protocol to redistribute routes from OSPF and the specified routes. The *metric* argument is in the range from 0–15. The options for the **match** keyword specify the types of internal or external routes that must be redistributed (you can specify more than one type).

Default	metric: 0 match: internal
Format	redistribute ospf [metric <i>metric</i>] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]
Mode	Router RIP Config

no redistribute ospf (Router RIP Config)

This command disables RIP protocol to redistribute routes from OSPF and the specified routes. The *metric* argument is in the range from 0–15.

Format	no redistribute ospf [metric <i>metric</i>] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]
Mode	Router RIP Config

show ip rip

M4250

M4350

This command displays information relevant to RIP on the switch.

Format	show ip rip
Modes	Privileged EXEC User EXEC

Term	Definition
RIP Admin Mode	Enable or disable.
Split Horizon Mode	None, simple or poison reverse.
Auto Summary Mode	Enable or disable. If enabled, groups of adjacent routes are summarized into single entries, in order to reduce the total number of entries. The default is enable.
Host Routes Accept Mode	Enable or disable. If enabled the router accepts host routes. The default is enable.
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.
Default Metric	The default metric of redistributed routes if one has already been set, or blank if not configured earlier. The valid values are 1 to 15.
Default Route Advertise	The default route.

show ip rip interface brief

M4250**M4350**

This command displays general information for each RIP interface. For this command to display successful results, routing must be enabled per interface (for example, through the **ip rip** command).

Format	show ip rip interface brief
Modes	Privileged EXEC User EXEC
Term	Definition
Interface	The interface.
IP Address	The IP source address used by the specified RIP interface.
Send Version	The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2
Receive Version	The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both
RIP Mode	The administrative mode of router RIP operation (enabled or disabled).
Link State	The mode of the interface (up or down).

show ip rip interface

M4250**M4350**

This command displays information related to a particular RIP interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* can be a number from 1–4093.

Format	show ip rip interface { <i>unit/slot/port</i> <i>vlan vlan-id</i> }
Modes	Privileged EXEC User EXEC

Term	Definition
Interface	The interface.
IP Address	The IP source address used by the specified RIP interface. This is a configured value.
Send Version	The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2. This is a configured value.
Receive Version	The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both. This is a configured value.
RIP Admin Mode	RIP administrative mode of router RIP operation; enable activates, disable de-activates it. This is a configured value.
Link State	Indicates whether the RIP interface is up or down. This is a configured value.
Authentication Type	The RIP Authentication Type for the specified interface. The types are none, simple, and encrypt. This is a configured value.

The following information will be invalid if the link state is down.

Term	Definition
Bad Packets Received	The number of RIP response packets received by the RIP process which were subsequently discarded for any reason.
Bad Routes Received	The number of routes contained in valid RIP packets that were ignored for any reason.
Updates Sent	The number of triggered RIP updates actually sent on this interface.

ICMP Throttling Commands

This section describes the commands you use to configure options for the transmission of various types of ICMP messages.

ip unreachable

M4250

M4350

Use this command to enable the generation of ICMP Destination Unreachable messages on an interface or range of interfaces. By default, the generation of ICMP Destination Unreachable messages is enabled.

Default	enable
Format	ip unreachable
Mode	Interface Config

no ip unreachable

Use this command to prevent the generation of ICMP Destination Unreachable messages.

Format	no ip unreachable
Mode	Interface Config

ip redirects

M4250

M4350

Use this command to enable the generation of ICMP Redirect messages by the switch. By default, the generation of ICMP Redirect messages is enabled. You can use this command to configure an interface, a range of interfaces, or all interfaces.

Default	enable
Format	ip redirects
Mode	Global Config Interface Config

no ip redirects

Use this command to prevent the generation of ICMP Redirect messages by the switch.

Format	no ip redirects
Mode	Global Config Interface Config

ipv6 redirects

M4250

M4350

Use this command to enable the generation of ICMPv6 Redirect messages by the switch. By default, the generation of ICMP Redirect messages is enabled. You can use this command to configure an interface, a range of interfaces, or all interfaces.

Default	enable
Format	ipv6 redirects
Mode	Interface Config

no ipv6 redirects

Use this command to prevent the generation of ICMPv6 Redirect messages by the switch.

Format	no ipv6 redirects

Mode	Interface Config

ip icmp echo-reply

M4250

M4350

Use this command to enable the generation of ICMP Echo Reply messages by the switch. By default, the generation of ICMP Echo Reply messages is enabled.

Default	enable

Format	ip icmp echo-reply

Mode	Global Config

no ip icmp echo-reply

Use this command to prevent the generation of ICMP Echo Reply messages by the switch.

Format	no ip icmp echo-reply

Mode	Global Config

ip icmp error-interval

M4250

M4350

Use this command to limit the rate at which IPv4 ICMP error messages are sent. The rate limit is configured as a token bucket, with two configurable parameters, *burst-size* and *burst-interval*.

The *burst-interval* specifies how often the token bucket is initialized with burst-size tokens. *burst-interval* is from 0 to 2147483647 milliseconds (msec). The *burst-size* is the number of ICMP error messages that can be sent during one *burst-interval*. The range is from 1 to 200 messages. To disable ICMP rate limiting, set the burst-interval to zero (0).

Default	burst-interval of 1000 msec. burst-size of 100 messages

Format	ip icmp error-interval <i>burst-interval</i> [<i>burst-size</i>]

Mode	Global Config

no ip icmp error-interval

Use the **no ip icmp error-interval** command to return the burst-interval and burst-size to their default values.

Format	no ip icmp error-interval
Mode	Global Config

IP Service Level Agreement Commands

The IP service-level agreement (SLA) feature let you monitor network performance between routers or from a router to a remote IP device. The metrics are collected by measuring ICMP response time and connectivity. This feature is deployed mostly in Enterprise networks on multi-homed customer edge devices, where there is a need to automatically switch to the next priority ISP in case of reachability issues with the current ISP.

ip sla

Use this command to start configuring an IP Service Level Agreements (SLAs) operation and let the CLI enter the IP SLA configuration mode. The *operation-number* argument specifies the IP SLA operation that is being configured. The range is from 1 to 128.

Default	No IP SLA is configured
Format	ip sla <i>operation-number</i>
Mode	Global Config

Usage guidelines:

Start configuring an IP SLA operation by using the **ip sla** command. This command specifies an identification number for the operation that is being configured. When you enter this command, the switch enters IP SLA configuration mode. This command is supported in IPv4 networks and also in IPv6 networks where IPv6 addresses are supported.

The maximum number of IP SLAs supported is 128 (IPv4 and IPv6 combined).

Once an operation is configured, it must be scheduled to be started (see the **ip sla schedule** command).

The configuration of an operation cannot be modified after an operation is scheduled to start. To modify the configuration of the operation after it is scheduled, the operation must either be stopped or be deleted using the **no ip sla** command, and then you can configure new operation parameters.

To display the current operational state of an IP SLA operation, use the **show ip sla** command in user EXEC or privileged EXEC mode.

The following example shows an operation 55 being configured as an ICMP Echo operation in an IPv4 network and being scheduled to start. In the following example, the **ip sla** command is used in an IPv4 network. (If SLA operation 55 is already configured and not scheduled, the CLI enters IP SLA configuration mode for operation 55. If the operation already exists and is already scheduled, this command fails.)

Command example:

```
(NETGEAR Switch) (config) # ip sla 55
(NETGEAR Switch) (config-ip-sla) # icmp-echo 172.16.1.175
(NETGEAR Switch) (config-ip-sla-echo) # exit
(NETGEAR Switch) (config-ip-sla) # exit
(NETGEAR Switch) (config) # ip sla schedule 55
```

no ip sla

Use this command to remove all the configuration information of an IP SLA operation, which also includes removing the schedule of the operation

Format	<code>no ip sla operation-number</code>

Mode	Global Config

ip sla schedule

M4250

M4350

After configuring an IP SLA operation, the IP SLA is in pending state and must be started using the **ip sla schedule** command. To stop the operation and place it in the default state (pending), use the **no ip sla schedule** command.

The *operation-number* argument specifies the IP SLA operation that is being schedules. The range is from 1 to 128.

Default	By default, the operation is placed in a pending state. In the pending state, the operation is enabled but does not actively probe and collect information.

Format	<code>ip sla schedule operation-number</code>

Mode	Global Config

Usage guidelines:

By default IP SLAs are not scheduled to start. After you create an IP SLA object with the **ip sla** command, you must start it (with an indefinite lifetime) with the **ip sla schedule** command. When you enter this command, the IP SLA operation transitions from the pending state to the active state and immediately begins probing and collecting information. You can stop the IP SLA probes by unconfiguring the IP SLA schedule with the **no ip sla schedule** command.

This command is supported in IPv4 networks and also for IPv6 networks where IPv6 addresses are supported.

The configuration of an operation cannot be modified after an operation is scheduled to start. To modify the configuration of the operation after it is scheduled, the operation must either be stopped or be deleted using the **no ip sla schedule** command, and then you can modify the operation. Or, you can delete the IP SLAs operation with the **no ip sla** command and then reconfigure the operation with the new operation parameters.

To display the current configuration settings of the operation, use the **show ip sla** command in user EXEC or privileged EXEC mode.

In the following example, operation 55 is configured as a ICMP Echo operation in an IPv4 network and is scheduled to start. The example shows the **ip sla schedule** command being used in an IPv4 network.

Command example:

```
(NETGEAR Switch) (config)# ip sla 55
(NETGEAR Switch) (config-ip-sla)#icmp-echo 172.16.1.175
(NETGEAR Switch) (config-ip-sla-echo)#exit
(NETGEAR Switch) (config-ip-sla)#exit
(NETGEAR Switch) (config)# ip sla schedule 55
```

no ip sla

Use this command to stop the IP SLA operation and place it in the default state (pending).

Format	no ip sla schedule <i>operation-number</i>

Mode	Global Config

track ip sla

M4250

M4350

Use this command to track the state of an IP SLA operation and to enter the tracking configuration mode.

This command lets the CLI enter the Track Config command mode.

Default	No objects and operations are tracked. By default, tracking uses reachability.

Format	track <i>object-number</i> ip sla <i>operation-number</i> [reachability state]

Mode	Global Config

Parameter	Description
<i>object-number</i>	The object to be tracked. The object is in the range of 1 to 128.
<i>operation-number</i>	The IP SLA operation to be tracked. The operation is in the range of 1 to 128.
reachability	Tracks if the route is reachable. Return code: - OK: The track state is Up. - OverThreshold: The track state is Up. - Timeout: The track state is Down.
state	Tracks the operation return code. Return code: - OK: The track state is Up. - OverThreshold: The track state is Up. - Timeout: The track state is Down.

Usage guidelines:

An operation return-code value is maintained by every IP SLA operation. This return code is interpreted by the tracking process. The return code may return OK, OverThreshold, or Timeout.

Two facets of an IP SLA operation can be tracked: reachability and state. The acceptance of the OverThreshold return code is the difference between these facets.

Tracking of a maximum of 128 (IPv4 and IPv6 combined) track objects is supported. If neither of the optional keywords (**reachability** or **state**) is specified in a configured **track ip sla** command, the default tracking type value **reachability** is used.

In the following example, the tracking process is configured to track the *state* of IP SLA operation 5.

Command example:

```
(NETGEAR Switch) (config) # track 2 ip sla 5 state
(NETGEAR Switch) (config-track) #
```

In the following example, the tracking process is configured to track the reachability of IP SLA operation 6.

Command example:

```
(NETGEAR Switch) (config) # track 3 ip sla 6 reachability
(NETGEAR Switch) (config-track) #
```

no track ip sla

Use this command to stop IP SLA tracking.

Format	no track <i>objection-number</i>

Mode	Global Config

delay (Track Config)

M4250

M4350

This command in Track Config mode specifies a delay for the switch to act on a track object if the reachability state changes.

To minimize flapping of the reachability (up/down) state, this command introduces a delay in seconds between the up and down state transitions. The delay time specifies the hold interval for up and down state transitions before the switch acts on the associated static routes.

The **track ip sla** command lets the CLI enter the Track Config command mode.

Default	None
Format	delay {up <i>seconds</i> [down <i>seconds</i>] [down <i>seconds</i>] up <i>seconds</i> }
Mode	Track Config
Parameter	Description
<i>up seconds</i>	The time to delay the notification for an up event. The value for <i>seconds</i> is from 0 to 180. The default is 0.
<i>down seconds</i>	The time to delay the notification of a down event. The value for <i>seconds</i> is from 0 to 180. The default is 0.

Command example:

In the following example, track object 10 is created and is associated with the IP SLAs operation 11 and then an up delay of 5 seconds and a down delay of 3 seconds is configured.

```
(NETGEAR Switch) (config)#track 10 ip sla 11
(NETGEAR Switch) (config-track)#delay up 5 down 3
```

no delay (Track Config)

This command in Track Config mode resets the delay for the switch to act on a track object if the reachability state changes.

Format	no delay
Mode	Track Config

IP SLA Configuration Commands

icmp-echo

M4250

M4350

Use this command in IP SLA configuration mode, to configure an IP Service Level Agreement (SLA) Internet Control Message Protocol (ICMP) echo operation.

Use the **ip sla** command to let the CLI enter the IP SLA configuration mode.

The **icmp-echo** command itself lets the CLI enter the IP SLA ICMP Echo configuration mode.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.,

Default	No IP SLAs operation type is configured.
Format	<code>icmp-echo destination-ip-address [source-interface {unit/slot/port vlan vlan-id}]</code>
Mode	IP SLA Config

Parameter	Description
<i>destination-ip-address</i>	The IPv4 or IPv6 destination address.
<i>unit/slot/port</i> or <i>vlan-id</i>	The source interface or VLAN ID for the operation.

Usage guidelines:

You must configure the type of IP SLA operation (ICMP echo) before you can configure any of the other parameters of the operation.

To change the operation values (the *destination-ip-address* argument, *interface-name* argument, or *vlan-id* argument) of an existing scheduled IP SLA ICMP echo operation, you must stop the IP SLA operation by using the **no ip sla schedule operation-number** command. Or, you can first delete the IP SLA operation (using the **no ip sla global** command) and then reconfigure the operation with the new operation parameters.

IP SLA ICMP echo operations support both IPv4 and IPv6 addresses.

Note: This command does not have a ‘No’ form. When you enter the `no ip sla operation-number` command to remove an IP SLA operation, the associated IP SLA ICMP Echo configuration is also removed.

Command example:

In the following example, IP SLA operation 12 is created and configured as an echo operation using the ICMP protocol and the destination IPv4 address 143.1.16.125.

```
(NETGEAR Switch) (config)#ip sla 12
(NETGEAR Switch) (config-ip-sla)#icmp-echo 143.1.16.125
(M4350-16V4C) (config-ip-sla-echo)#
```

Command example:

In the following example, IP SLAs operation 13 is created and configured as an echo operation using the ICMP protocol and the destination IPv6 address 3001:CD6:200::1.

```
(NETGEAR Switch) (config)#ip sla 13
(NETGEAR Switch) (config-ip-sla)#icmp-echo 3001:CD6:200::1
(NETGEAR Switch) (config-ip-sla-echo)#
```

frequency (IP SLA ICMP Echo Config)

M4250

M4350

Use the **icmp-echo** command to let the CLI enter the IP SLA ICMP Echo configuration mode.

This command sets the rate at which a specified IP Service Level Agreement (SLA) operation repeats. The *seconds* argument specifies the number of seconds between the IP SLA operations, which can range from 1 to 3600 seconds.

Default	60 seconds
Format	<i>frequency seconds</i>
Mode	IP SLA ICMP Echo Config

Usage guidelines

A single IP SLA operation repeats at a frequency for the duration of the operation. For example, an ICMP echo operation with a frequency of 60 sends an ICMP Echo Request packet once every 60 seconds for the duration of the operation. This packet is sent when the operation starts, and then is sent again 60 seconds later.

If an individual IP SLA operation takes longer to execute than the specified frequency value, a statistics counter called “busy” is incremented rather than that the operation is immediately repeated.

We recommend the following order for configuring the **frequency**, **timeout**, and **threshold** commands of an IP SLA ICMP Echo operation:

1. **frequency** *seconds*
2. **timeout** *milliseconds*
3. **threshold** *milliseconds*

Note: We recommend that you do not set the frequency value to less than 60 seconds because the potential overhead from numerous active operations could significantly affect network performance.

This command is supported in IPv4 and IPv6 networks.

Command example:

The following example shows how to configure an IP SLA ICMP echo operation (operation 11) to repeat every 80 seconds. This example shows the frequency (IP SLA) command being used in an IPv4 network in ICMP echo configuration mode within IP SLA configuration mode:

```
(NETGEAR Switch) (config) #ip sla 11
(NETGEAR Switch) (config-ip-sla) #icmp-echo 203.15.10.145
(NETGEAR Switch) (config-ip-sla-echo) #frequency 80
```

no frequency (IP SLA ICMP Echo Config)

This command returns the frequency to the default value of 60 seconds.

Format	no frequency
Mode	IP SLA ICMP Echo Config

timeout (IP SLA ICMP Echo Config)

M4250

M4350

Use the **icmp-echo** command to let the CLI enter the IP SLA ICMP Echo configuration mode.

This command sets the period that an IP Service Level Agreement (SLA) operation waits for a response from its request packet. The *milliseconds* argument specifies the number of milliseconds that the operation waits to receive a response from its request packet. The range can be from 50 to 300000 milliseconds.

Base the *milliseconds* argument on the sum of both the maximum round-trip time (RTT) value for the packets and the processing time of the IP SLAs operation.

Default	5000 milliseconds
Format	<code>timeout milliseconds</code>
Mode	IP SLA ICMP Echo Config

Usage guidelines

We recommend that you base the *milliseconds* argument on the sum of both the maximum round-trip time (RTT) for the packets and the processing time of the IP SLA operation. The *milliseconds* argument cannot be greater than the *seconds* argument in the **frequency** command.

We recommend the following order for configuring the **frequency**, **timeout**, and **threshold** commands of an IP SLA ICMP Echo operation:

1. **frequency** *seconds*
2. **timeout** *milliseconds*
3. **threshold** *milliseconds*

This command is supported in IPv4 and IPv6 networks.

Command example:

In the following example, the time-out value for an IP SLAs operation 11 is set for 2500 ms.

```
(NETGEAR Switch) (config) #ip sla 11
(NETGEAR Switch) (config-ip-sla) #icmp-echo 152.17.10.145
(NETGEAR Switch) (config-ip-sla-echo) #timeout 2500
```

no timeout (IP SLA ICMP Echo Config)

This command returns the time-out to the default value of 5000 milliseconds.

Format	<code>no timeout</code>
Mode	IP SLA ICMP Echo Config

threshold (IP SLA ICMP Echo Config)

M4250

M4350

Use the **icmp-echo** command to let the CLI enter the IP SLA ICMP Echo configuration mode.

This command sets the upper threshold value for calculating network monitoring statistics that are created by an IP SLA operation. The *milliseconds* argument specifies the number of milliseconds for the upper threshold. The range can be from 50 to 60000 milliseconds.

Default	5000 milliseconds
Format	<code>threshold milliseconds</code>
Mode	IP SLA ICMP Echo Config

Usage guidelines

The *milliseconds* argument cannot be greater than the *milliseconds* argument in the **timeout** command.

We recommend the following order for configuring the **frequency**, **timeout**, and **threshold** commands of an IP SLA ICMP Echo operation:

1. **frequency** *seconds*
2. **timeout** *milliseconds*
3. **threshold** *milliseconds*

This command is supported in IPv4 and IPv6 networks.

Command example:

In the following example, the threshold for the IP SLA ICMP echo operation is set to 3500 milliseconds.

```
(NETGEAR Switch) (config) #ip sla 11
(NETGEAR Switch) (config-ip-sla) #icmp-echo 152.17.10.145
(NETGEAR Switch) (config-ip-sla-echo) #threshold 3500
```

no threshold (IP SLA ICMP Echo Config)

This command returns the threshold to the default value of 5000 milliseconds.

Format	<code>no threshold</code>
Mode	IP SLA ICMP Echo Config

vrf (IP SLA ICMP Echo Config)

M4250

M4350

Use the **icmp-echo** command to let the CLI enter the IP SLA ICMP Echo configuration mode.

This command allows reachability monitoring within a virtual private network (VPN) using IP an Service Level Agreements (SLA) operation.

The *vrf-name* argument is the VPN routing and forwarding (VRF) name.

Default	By default, every IP SLA operation is used to monitor in the default VRF.

Format	<code>threshold vrf-name</code>

Mode	IP SLA ICMP Echo Config

Usage guidelines

Use this command only if the response time over a VPN tunnel must be measured.

This command is supported in IPv4 networks only.

Command example:

This example shows how test traffic can be sent in an existing VPN tunnel between two endpoints.

```
(NETGEAR Switch) (config)#ip sla 11
(NETGEAR Switch) (config-ip-sla)#icmp-echo 35.1.10.2
(NETGEAR Switch) (config-ip-sla-echo)#vrf vpn1
```

`no vrf` (IP SLA ICMP Echo Config)

This command removes a VRF association.

Format	<code>no vrf</code>

Mode	IP SLA ICMP Echo Config

`show ip sla configuration`

M4250

M4350

This command displays the configuration values (including all defaults) for all or a specific IP SLAs operation. The value for the *operation number* argument can be from 1 to 128.

Format	<code>show ip sla configuration [operation-number]</code>

Mode	User EXEC Privileged EXEC

Command example:

The following command output displays IP SLAs operations in an IPv4 network.

```
(NETGEAR Switch)#show ip sla configuration 3

Entry number: 3
Type of operation: echo
Target address/Source address: 1.1.1.1/0.0.0.0
```

```

Operation timeout (milliseconds): 5000
Vrf Name:
Schedule:
    Next Scheduled Start Time: Start Time already passed
    Operation frequency (seconds): 60
    Life: Forever
Threshold (milliseconds): 5000

```

Command example:

The following command output displays IP SLAs operations in an IPv6 network.

```

(NETGEAR Switch)#show ip sla configuration 5

Entry number: 3
Type of operation: echo
Target address/Source address: 2001:DB8:100::1/2001:0DB8:200::FFFE
Operation timeout (milliseconds): 5000
Vrf Name:
Schedule:
    Next Scheduled Start Time: Pending Trigger
    Operation frequency (seconds): 60
    Life: Forever
Threshold (milliseconds): 5000

```

show ip sla statistics**M4250****M4350**

This command displays the statistics and the current operational status of all or a specific IP SLA operation.

This command also shows the current state of IP SLAs operations, including whether the operation is active and also the monitoring data returned for the last (most recently completed) operation.

Format	show ip sla statistics [<i>operation-number</i>] [<i>details</i>]

Mode	User EXEC Privileged EXEC

Parameter	Description
<i>operation-number</i>	(Optional) The operation number argument, which can be from 1 to 128.
detail	(Optional) Display statistics and the operational status in greater detail.

Command example:

```
(NETGEAR Switch)# show ip sla statistics details
```

```
Round Trip Time (RTT) for          Index 1
Type of operation: icmp-echo
    Latest RTT: 1 ms
Latest operation start time: 47 milliseconds
Latest operation return code: OK
Over thresholds occurred: FALSE
Number of successes: 14
Number of failures: 0
Operation time to live: Forever
Operational state of entry: Active
```

clear ip sla statistics

M4250

M4350

Use this command to clear IP SLA statistical information for all or a specific IP SLA operation.

The optional *operation-number* argument limits the clearing to a specific IP SLA operation

Format	clear ip sla statistics [<i>operation-number</i>]

Mode	Privileged EXEC

show ip route track-table

M4250

M4350

This command displays information about all tracked IPv4 static routes.

Format	show ip route track-table

Mode	User EXEC Privileged EXEC

Command example:

```
(NETGEAR Switch)#show ip route track-table
```

show ipv6 route track-table

M4250

M4350

This command displays information about all tracked IPv6 static routes.

Format	show ipv6 route track-table

Mode	User EXEC Privileged EXEC

Command example:

```
(NETGEAR Switch)#show ipv6 route track-table
```

```
ipv6 route 2001:B66::/32 4001::1 track 15 state is [up]
```

show track

M4250

M4350

This command displays detailed information about all track objects or for a specific track object. You can also use the command to display brief information about all track objects or about track objects that are associated with a specific IP SLA operation.

Format	show track [brief <i>track-number</i> {ip sla <i>operation-number</i> }]

Mode	Privileged Config

Parameter	Description
brief	Displays brief information for all track objects.
<i>track-number</i>	The track object's number from 1 to 128 for which detailed information must be displayed.
ip sla <i>operation-number</i>	The IP SLA operation number for which information about the associated track-objects must be displayed.

Command example:

The following example shows detailed information for all track objects.

```
(NETGEAR Switch)#show track
```

```
Track 10
  IP SLA 1 reachability
  Reachability is Up
    1 change, last change 01:12:36
  Delay up 5 secs, down 5 secs
```

```
Latest operation return code: OK
Latest RTT (milliseconds) 1500
```

```
Track 11
  IP SLA 2 state
  State is Up
    1 change, last change 00:41:55
  Delay up 10 secs, down 10 secs
  Latest operation return code: OK
  Latest RTT (milliseconds) 1000
```

```
Track 13
  IP SLA 1 state
  State is Up
    1 change, last change 00:34:08
  Delay up 5 secs, down 5 secs
  Latest operation return code: OK
  Latest RTT (milliseconds) 1500
```

Command example:

The following example shows detailed information for track object 10.

```
(NETGEAR Switch)#show track 10
```

```
Track 10
  IP SLA 1 reachability
  Reachability is Up
    1 change, last change 01:12:36
  Delay up 5 secs, down 5 secs
  Latest operation return code: OK
  Latest RTT (milliseconds) 1500
```

Command example:

The following example shows brief information for all track objects associated with IP SLA operation 1.

```
(NETGEAR Switch)#show track ip sla 1
```

Track	Object	Parameter	Value	Last Change
10	ip sla 1	reachability	Up	01:12:36
13	ip sla 1	state	Up	00:34:08

Command example:

The following example shows brief information for all track objects.

```
(NETGEAR Switch)#show track brief
```

Track	Object		Parameter	Value	Last Change
10	ip sla	1	reachability	Up	01:12:36
11	ip sla	2	state	Up	00:41:55
13	ip sla	1	state	Up	00:34:08

9

Captive Portal Commands

This section describes the CLI commands that you can use to manage the captive portal features on the switch. The chapter contains the following sections:

- [Captive Portal Global Commands](#)
- [Captive Portal Configuration Commands](#)
- [Captive Portal Status Commands](#)
- [Captive Portal Client Connection Commands](#)
- [Captive Portal Interface Commands](#)
- [Captive Portal Local User and User Group Commands](#)

Captive Portal Global Commands

The commands in this section enable you to configure the captive portal settings that affect the captive portal feature on the switch and all captive portal instances.

For information about user and user group commands in the Captive Portal Configuration mode, see [Captive Portal Local User and User Group Commands](#).

captive-portal

M4250

M4350

Use this command to enter the Captive Portal Configuration mode.

This command lets the CLI enter the Captive Portal configuration mode.

Format	captive-portal
Mode	Global Config

enable (Captive Portal Config)

M4250

M4350

This command globally enables the captive portal feature on the switch.

Default	Disable
Format	enable
Mode	Captive Portal Config

no enable (Captive Portal Config)

The **no enable** command disables the captive portal functionality.

Format	no enable
Mode	Captive Portal Config

http port (Captive Portal Config)

M4250**M4350**

This command configures an additional HTTP port. Valid port numbers are in the range of 0-65535, excluding port numbers 80 and 443 which are reserved. The HTTP port default is 0 which denotes no additional port and the default port (80) is used.

Default	0
Format	<code>http port <i>port-number</i></code>
Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch) (Config-CP) #http port 8080
(NETGEAR Switch) (Config-CP) #no http port
```

no http port (Captive Portal Config)

This command removes the specified additional HTTP port.

Format	<code>no http port <i>port-number</i></code>
Mode	Captive Portal Config

https port (Captive Portal Config)

M4250**M4350**

This command configures an additional HTTPS secure port. The HTTPS secure port default is 0 which denotes no additional port and the default port (443) is used. Port number 80 is reserved.

Default	0
Format	<code>https port <i>port-number</i></code>
Mode	Captive Portal Config

Parameter	Description
port-num	Port number in the range of 0-65535.

Command example:

```
(NETGEAR Switch) (Config-CP) #https port 60000
(NETGEAR Switch) (Config-CP) #no https port
```

no https port (Captive Portal Config)

This command set the HTTPS secure port to the default.

Format	no https port <i>port-number</i>

Mode	Captive Portal Config

authentication timeout (Captive Portal Config)

M4250

M4350

This command configures the authentication time-out. If the captive portal user does not enter valid credentials within this time limit, the authentication page needs to be served again in order for the client to gain access to the network. The *seconds* variable is the authentication time-out and is a number in the range of 60-600 seconds.

Default	300

Format	authentication timeout <i>seconds</i>

Mode	Captive Portal Config

no authentication timeout (Captive Portal Config)

This command sets the authentication timeout to the default value.

Format	no authentication timeout

Mode	Captive Portal Config

trapflags (Captive Portal Config)

M4250

M4350

This command enables captive portal SNMP traps. If no parameters are specified, then all traps are enabled. SNMP traps can also be enabled individually by supplying the optional parameters.

The **client-auth-failure** option allows the SNMP agent to send a trap when a client attempts to authenticate with a captive portal but is unsuccessful.

The **client-connect** option allows the SNMP agent to send a trap when a client authenticates with and connects to a captive portal.

The **client-db-full** option allows the SNMP agent to send a trap each time an entry cannot be added to the client database because it is full.

The **client-disconnect** option allows the SNMP agent to send a trap when a client disconnects from a captive portal.

Default	Disabled
Format	trapflags [client-auth-failure client-connect client-db-full client-disconnect]
Mode	Captive Portal Config

no trapflags (Captive Portal Config)

This command disables all captive portal SNMP traps when no parameters are specified. The optional parameters specify individual traps to disable.

Format	no trapflags [client-auth-failure client-connect client-db-full client-disconnect]
Mode	Captive Portal Config

snmp-server enable traps captive-portal

M4250

M4350

This command globally enables the captive portal traps. The specific captive portal traps are configured using the **trapflags** command in Captive Portal Config mode.

Default	Disable
Format	snmp-server enable traps captive-portal
Mode	Global Config

no snmp-server enable traps captive-portal

This command globally disables all the captive portal traps.

Format	no snmp-server enable traps captive-portal
Mode	Global Config

show captive-portal

M4250

M4350

This command reports status of the captive portal feature.

Format	show captive-portal
Mode	Privileged EXEC

Term	Description
Administrative Mode	Shows whether the CP is enabled.
Operational Status	Indicates whether the CP operational status is enabled or disabled.
Disable Reason	If CP is disabled, this field displays the reason, which can be None, Administratively Disabled, No IPv4 Address, or Routing Enabled, but no IPv4 routing interface.
Captive Portal IP Address	Shows the IP address that the captive portal feature uses.

show captive-portal status

M4250

M4350

This command reports status of all captive portal instances in the system.

Format	<code>show captive-portal status</code>
Mode	Privileged EXEC

Term	Description
Additional HTTP Port	Displays the port number of the additional HTTP port configured for traffic. A value of 0 indicates that only port 80 is configured for HTTP traffic.
Additional HTTP Secure Port	Displays the port number of the additional HTTPS secure port. A value of 0 indicates no additional port and the default port (443) is used.
Peer Switch Statistics Reporting Interval	Displays the interval at which statistics are reported in the Cluster Controller. The reporting interval is in the range of 0, 15-3600 seconds where 0 disables statistical reporting.
Authentication Timeout	Displays the number of seconds to keep the authentication session open with the client. When the timeout expires, the switch disconnects any active TCP or SSL connection with the client.
Supported Captive Portals	Shows 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.
Local Supported Users	Shows the number of users that can be added and configured using the local user database.
Configured Local Users	Shows the number of users that are configured from the local user database.

Term	Description
System Supported Users	Shows the total number of authenticated users that the system can support.
Authenticated Users	Shows the number of users currently authenticated to all captive portal instances on this switch.

Command example:

```
(NETGEAR Switch) #show captive-portal status
Additional HTTP Port..... 0
Additional HTTP Secure Port..... 0
Peer Switch Statistics Reporting Interval..... 120
Authentication Timeout..... 300
Supported Captive Portals..... 10
Configured Captive Portals..... 1
Active Captive Portals..... 0
Local Supported Users..... 128
Configured Local Users..... 0
System Supported Users..... 1024
Authenticated Users..... 0
```

show captive-portal trapflags**M4250****M4350**

This command shows which captive portal SNMP traps are enabled. The **show trapflags** command shows the global captive portal traps configuration. For more information, see the sample output of [show trapflags \(M4250 series switch\)](#) on page 181.

Format	<code>show captive-portal trapflags</code>

Mode	Privileged EXEC

Term	Description
Client Authentication Failure Traps	Shows whether the SNMP agent sends a trap when a client attempts to authenticate with a captive portal but is unsuccessful.
Client Connection Traps	Shows whether the SNMP agent sends a trap when a client authenticates with and connects to a captive portal.
Client Database Full Traps	Shows whether the SNMP agent sends a trap each time an entry cannot be added to the client database because it is full.
Client Disconnection Traps	Shows whether the SNMP agent sends a trap when a client disconnects from a captive portal.

Captive Portal Configuration Commands

The commands in this section are related to captive portal configurations.

configuration (for captive portal)

M4250

M4350

Use the **captive-portal** command to let the CLI enter the Captive Portal Configuration mode. From the Captive Portal Configuration mode, use the **configuration** command to let the CLI enter the Captive Portal Instance mode.

The captive portal configuration, identified by CP ID 1, is the default CP configuration. You can create up to nine additional captive portal configurations. The system supports a total of ten CP configurations. The Captive Portal ID *cp-id* variable is a number in the range of 1-10.

Format	<code>configuration cp-id</code>
Mode	Captive Portal Config

no configuration

This command deletes a captive portal configuration. The command fails if interfaces are associated with this configuration. The default captive portal configuration cannot be deleted. The Captive Portal ID *cp-id* variable is a number in the range of 1-10.

Format	<code>no configuration cp-id</code>
Mode	Captive Portal Config

enable (Captive Portal Instance)

M4250

M4350

This command enables a captive portal configuration.

Default	Enable
Format	<code>enable</code>
Mode	Captive Portal Instance

no enable

This command disables a captive portal configuration.

Format	no enable
Mode	Captive Portal Instance

name

M4250

M4350

This command configures the name for a captive portal configuration. The *cp-name* can contain up to 32 alphanumeric characters.

Format	name <i>cp-name</i>
Mode	Captive Portal Instance

no name

This command removes the name for a captive portal configuration.

Format	no name
Mode	Captive Portal Instance

protocol

M4250

M4350

This command configures the protocol for a captive portal configuration. The CP can use HTTP or HTTPS protocols.

Default	https
Format	protocol {http https}
Mode	Captive Portal Instance

no protocol

This command removes the protocol for a captive portal configuration.

Format	no protocol
Mode	Captive Portal Instance

verification

M4250**M4350**

This command configures the verification mode for a captive portal configuration. The type of user verification to perform can be one of the following:

- **guest**. The user does not need to be authenticated by a database.
- **local**. The switch uses a local database to authenticated users.
- **radius**. The switch uses a database on a remote RADIUS server to authenticate users.

Default	guest
Format	verification {guest local radius}
Mode	Captive Portal Instance

no verification

This command removes the verification mode for a captive portal configuration.

Format	no verification
Mode	Captive Portal Instance

group

M4250**M4350**

This command assigns a group ID to a captive portal configuration. Each Captive Portal configuration must contain at least one group ID. The *group-id* can have a number in the 1–1024 range. Group ID 1 is the default.

Default	group-ID 1
Format	group <i>group-id</i>
Mode	Captive Portal Instance

no group

This command removes the group ID for a captive portal configuration.

Format	no group
Mode	Captive Portal Instance

radius-auth-server

M4250

M4350

Use this command to configure a captive portal configuration RADIUS authentication server.

Default	Disable
Format	<code>radius-auth-server server-name</code>
Mode	Captive Portal Instance

no radius-auth-server

This command disables a captive portal configuration RADIUS authentication server.

Format	<code>no radius-auth-server</code>
Mode	Captive Portal Instance

redirect

M4250

M4350

This command enables the redirect mode for a captive portal configuration.

Default	Disable
Format	<code>redirect</code>
Mode	Captive Portal Instance

no redirect

This command disables the redirect mode for a captive portal configuration.

Format	<code>no redirect</code>
Mode	Captive Portal Instance

redirect-url

M4250

M4350

Use this command to specify the URL to which a newly authenticated client is redirected if the URL Redirect Mode is enabled. This command is only available if the redirect mode is enabled.

Format	<code>redirect-url url</code>

Mode	Captive Portal Instance

no redirect-url

This command removes the URL to which a newly authenticated client is redirected if the URL Redirect Mode is enabled.

Format	<code>no redirect-url</code>

Mode	Captive Portal Instance

max-bandwidth-up

M4250

M4350

This command configures the maximum rate at which a client can send data into the network.

Default	0

Format	<code>max-bandwidth-up rate</code>

Mode	Captive Portal Config

Parameter	Description
rate	Rate in bps. 0 indicates limit not enforced.

no max-bandwidth-up

This command sets the maximum rate at which a client can send data into the network to the default.

Format	<code>no max-bandwidth-up</code>

Mode	Captive Portal Instance

max-bandwidth-down

M4250**M4350**

This command configures the maximum rate at which a client can receive data from the network. If the value is set to 0, the rate is not enforced.

Default	0
Format	max-bandwidth-down <i>rate</i>
Mode	Captive Portal Instance
Parameter	Description
rate	Rate in bps. 0 indicates that the limit not enforced.

no max-bandwidth-down

This command sets to the default the maximum rate at which a client can receive data from the network.

Format	no max-bandwidth-down
Mode	Captive Portal Instance

max-input-octets

M4250**M4350**

This command configures the maximum number of octets the user is allowed to transmit. After this limit has been reached the user will be disconnected. If the value is set to 0, the limit is not enforced.

Default	0
Format	max-input-octets <i>bytes</i>
Mode	Captive Portal Instance
Parameter	Description
bytes	Input octets in bytes. 0 indicates that the limit not enforced.

no max-input-octets

This command sets to the default the maximum number of octets the user is allowed to transmit.

Format	no max-input-octets

Mode	Captive Portal Instance

max-output-octets

M4250

M4350

This command configures the maximum number of octets the user is allowed to receive. After this limit is reached, the user is disconnected. If the value is set to 0, the limit is not enforced.

Default	0

Format	max-output-octets <i>bytes</i>

Mode	Captive Portal Instance

Parameter	Description

bytes	Output octets in bytes. 0 indicates that the limit not enforced.

no max-output-octets

This command sets to the default the maximum number of octets the user is allowed to receive.

Format	no max-output-octets

Mode	Captive Portal Instance

max-total-octets

M4250

M4350

This command configures the maximum number of octets a user is allowed to transfer, that is, the sum of octets transmitted and received. After this limit is reached, the user is disconnected. If the value is set to 0, then the limit is not enforced.

Default	0

Format	max-total-octets <i>bytes</i>

Mode	Captive Portal Instance

Parameter	Description
bytes	Total octets in bytes. 0 indicates limit not enforced.

no max-total-octets

This command sets to the default the maximum number of octets the user is allowed to transfer, that is, the sum of octets transmitted and received.

Format	no max-total-octets
Mode	Captive Portal Instance

session-timeout (Captive Portal Instance)

M4250

M4350

This command configures the session time-out for a captive portal configuration. The *timeout* variable is a number that represents the session time-out in seconds. Use 0 to indicate that the time-out is not enforced.

Default	0
Format	session-timeout <i>timeout</i>
Mode	Captive Portal Instance

no session-timeout

Use this command to set the session time-out for a captive portal configuration to the default value.

Format	no session-timeout
Mode	Captive Portal Instance

idle-timeout

M4250

M4350

This command configures the idle time-out for a captive portal configuration. The *timeout* variable is a number that represents the idle time-out in seconds. Use 0 to indicate that the time-out is not enforced.

Default	0
Format	<code>idle-timeout timeout</code>
Mode	Captive Portal Instance

no idle-timeout

Use this command to set the idle time-out for a captive portal configuration to the default value.

Format	<code>no idle-timeout</code>
Mode	Captive Portal Instance

locale

M4250

M4350

This command is not intended to be a user command. The administrator must use the Main user interface to create and customize captive portal web content. The command is primarily used by the **show running config** command and process as it provides the ability to save and restore configurations using a text-based format.

Format	<code>locale web-id</code>
Mode	Captive Portal Instance

interface (Captive Portal Instance)

M4250

M4350

This command associates an interface with a captive portal configuration. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument `slot/port`.
- For an M4350 series switch, use the argument `unit/slot/port`, as shown in the command format.

Format	<code>interface unit/slot/port</code>
Mode	Captive Portal Instance

no interface (Captive Portal Instance)

This command removes the association between an interface and a captive portal configuration.

Format	<code>no interface unit/slot/port</code>

Mode	Captive Portal Instance

block

M4250

M4350

This command blocks all traffic for a captive portal configuration.

Format	<code>block</code>

Mode	Captive Portal Instance

no block

This command unblocks all traffic for a captive portal configuration.

Format	<code>no block</code>

Mode	Captive Portal Instance

clear (Captive Portal Instance Config)

M4250

M4350

This command sets the configuration for this instance to the default values.

Format	<code>clear</code>

Mode	Captive Portal Instance

user-logout

M4250

M4350

This command enables the ability for an authenticated user to de-authenticate from the network. This command is configurable for a captive portal configuration.

Format	<code>user-logout</code>

Mode	Captive Portal Instance

no user-logout

This command removes the association between an interface and a captive portal configuration.

Format	no user-logout
Mode	Captive Portal Instance

background-color

M4250

M4350

Use this command to customize the background color of the Captive Portal authentication page using a well-known color name or RGB value. For example, red or RGB hex-code, that is, #FF0000. The range of *color-code* is 1-32 characters.

Default	#BFBFBF
Format	background-color <i>color-code</i>
Mode	Captive Portal Instance

no background-color

This command reverts the background color of the Captive Portal authentication page to the default color.

Format	no background-color
Mode	Captive Portal Instance

foreground-color

M4250

M4350

Use this command to customize the foreground color of the Captive Portal authentication page using a well-known color name or RGB value. For example, red or RGB hex-code, that is, #FF0000. The range of *color-code* is 1-32 characters.

Default	#999999
Format	foreground-color <i>color-code</i>
Mode	Captive Portal Instance

no foreground-color

This command reverts the foreground color of the Captive Portal authentication page to the default color.

Format	no foreground-color

Mode	Captive Portal Instance

separator-color

M4250

M4350

Use this command to customize the separator bar color of the Captive Portal authentication page using a well-known color name or RGB value. For example, red or RGB hex-code; that is, #FF0000. The range of *color-code* is 1-32 characters.

Default	#BFBFBF

Format	separator-color <i>color-code</i>

Mode	Captive Portal Instance

no separator-color

This command reverts the separator bar color of the Captive Portal authentication page to the default color.

Format	no separator-color

Mode	Captive Portal Instance

Captive Portal Status Commands

Use the commands in this section to view information about the status of one or more captive portal instances.

show captive-portal configuration

M4250

M4350

This command displays the operational status of a captive portal configuration. The *cp-id* variable is the captive portal ID, which ranges from 1-10.

Format	show captive-portal configuration <i>cp-id</i>
Mode	Privileged EXEC
Term	Description
CP ID	Shows the captive portal ID.
CP Name	Shows the captive portal name.
Operational Status	Shows whether the captive portal is enabled or disabled.
Disable Reason	If the captive portal is disabled, this field indicates the reason.
Blocked Status	Shows the blocked status, which is Blocked or Not Blocked.
Authenticated Users	Shows the number of authenticated users connected to the network through this captive portal.
Configured Locales	Shows the number of locales defined for this captive portal.

show captive-portal configuration interface

M4250

M4350

This command displays information for all interfaces assigned to a captive portal configuration or a specific interface assigned to a captive portal configuration. The *cp-id* variable is the captive portal ID, which ranges from 1-10.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format `show captive-portal configuration cp-id interface [unit/slot/port]`

Mode Privileged EXEC

Term	Description
CP ID	Shows the captive portal ID.
CP Name	Shows the captive portal name.
Interface	Shows the interface
Interface Description	Describes the interface.
Operational Status	Shows whether the captive portal is enabled or disabled
Block Status	Shows the blocked status, which is Blocked or Not Blocked.
If you specify a single interface, the following additional information displays:	
Disable Reason	If the captive portal is disabled, this field indicates the reason.
Authenticated Users	Shows the number of authenticated users connected to the network through this captive portal.

show captive-portal configuration status

M4250

M4350

This command displays information of all configured captive portal configurations or a specific captive portal configuration. The *cp-id* variable is the captive portal ID, which ranges from 1-10.

Format `show captive-portal configuration cp-id status`

Mode Privileged EXEC

Term	Description
CP ID	Shows the captive portal ID.
CP Name	Shows the captive portal name.
CP Mode	Shows whether the CP is enabled or disabled.
Protocol Mode	Shows the current connection protocol, which is either HTTP or HTTPS.
Verification Mode	Shows the current account type, which is Guest, Local, or RADIUS.
URL Redirect Mode	Indicates whether the Redirect URL Mode is enabled or disabled.

Term	Description
Max Bandwidth Up (bytes/sec)	The maximum rate in bytes per second (bps) at which a client can send data into the network.
Max Bandwidth Down (bytes/sec)	The maximum rate in bps at which a client can receive data from the network.
Max Input Octets (bytes)	The maximum number of octets the user is allowed to transmit.
Max Output Octets (bytes)	The maximum number of octets the user is allowed to receive.
Max Total Octets (bytes)	The maximum number of octets the user is allowed to transfer, i.e., the sum of octets transmitted and received.
Session Timeout (seconds)	Shows 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. A value of 0 means that the user does not have a session Timeout limit.
Idle Timeout (seconds)	Shows the number of seconds the user can remain idle before the switch automatically logs the user out. A value of 0 means that the user will not be logged out automatically.

show captive-portal configuration locales

M4250

M4350

This command displays locales associated with a specific captive portal configuration. The *cp-id* variable is the captive portal ID, which ranges from 1-10.

Format	<code>show captive-portal configuration cp-id locales</code>
Mode	Privileged EXEC
Term	Description
Locale Code	Two-letter abbreviation for languages.
Locale Link	The names of the languages.

Captive Portal Client Connection Commands

Use the commands in this section to view information about the clients connected to the captive portals configured on the switch.

show captive-portal client status

M4250

M4350

This command displays client connection details or a connection summary for connected captive portal users. Use the optional *macaddr* keyword, which is the MAC address of a client, to view additional information about that client.

Format	show captive-portal client [<i>macaddr</i>] status
Mode	Privileged EXEC
Term	Description
Client MAC Address	Identifies the MAC address of the wireless client (if applicable).
Client IP Address	Identifies the IP address of the wireless client (if applicable).
Protocol Mode	Shows the current connection protocol, which is either HTTP or HTTPS.
Verification Mode	Shows the current account type, which is Guest, Local, or RADIUS.
Session Time	Shows the amount of time that has passed since the client was authorized.
If you specify a client MAC address, the following additional information displays:	
CP ID	Shows the captive portal ID the connected client is using.
CP Name	Shows the name of the captive portal the connected client is using.
Interface	Valid unit and port number separated by a forward slash.
Interface Description	Describes the interface.
User Name	Displays the user name (or Guest ID) of the connected client.
If cluster support is available, the following fields display:	
Switch MAC Address	Identifies the MAC address of the switch (if applicable).

Term	Description
Switch IP Address	Identifies the IP address of the switch (if applicable).
Switch Type (local or peer)	Shows the current switch type, which is local or peer.

show captive-portal client status

M4250

M4350

This command displays client connection details or a connection summary for connected captive portal users. Use the optional *macaddr* argument, which is the MAC address of a client, to view additional information about the client.

Format	<code>show captive-portal client [macaddr] status</code>
Mode	Privileged EXEC

Term	Description
Client MAC Address	The MAC address of the wireless client (if applicable).
Client IP Address	The IP address of the wireless client (if applicable).
Protocol Mode	The connection protocol, which is either HTTP or HTTPS
Verification Mode	The account type, which is Guest, Local, or RADIUS.
Session Time	The period that has passed since the client was authorized.

If you specify a client MAC address, the following additional information displays.

Term	Description
CP ID	The captive portal ID that the connected client is using.
CP Name	The name of the captive portal that the connected client is using.
Interface	The interface number.
Interface Description	The interface description.
User Name	The user name (or Guest ID) of the connected client.

If cluster support is available, the following fields display.

Term	Description
Switch MAC Address	The MAC address of the switch (if applicable).
Switch IP Address	The IP address of the switch (if applicable).
Switch Type (local or peer)	The switch type, which is local or peer.

show captive-portal interface client status

M4250

M4350

This command displays information about clients authenticated on all interfaces or a specific interface.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show captive-portal interface [<i>unit/slot/port</i>] client status
Mode	Privileged EXEC
Term	Description
Interface	The interface number.
Interface Description	Describes the interface.
Client MAC Address	Identifies the MAC address of the wireless client (if applicable).

If you specify a single interface, the following additional information displays.

Term	Description
Client IP Address	Identifies the IP address of the wireless client (if applicable).
CP ID	Shows the captive portal ID the connected client is using.
CP Name	Shows the name of the captive portal the connected client is using.
Protocol	Shows the current connection protocol, which is either HTTP or HTTPS.

Term	Description
Verification	Shows the current account type, which is Guest, Local, or RADIUS.
User Name	Displays the user name (or Guest ID) of the connected client.

show captive-portal configuration client status

M4250

M4350

This command displays the clients authenticated to all captive portal configurations or a specific configuration. The optional *cp-id* variable is the captive portal ID, which ranges from 1-10. Use the optional **client** keyword to display client information.

Format	show captive-portal configuration [<i>cp-id</i>] [<i>client</i>] status
Mode	Privileged EXEC

Term	Description
CP ID	The captive portal ID the connected client is using.
CP Name	The name of the captive portal the connected client is using.
Mode	Shows if the captive portal is enabled or disabled
Protocol	The protocol (HTTP or HTTPS) that is used for the captive portal.
Verification	The type of verification, such as Guest.

If you use the optional **client** keyword, the following information displays.

Term	Description
CP ID	The captive portal ID the connected client is using.
CP Name	The name of the captive portal the connected client is using.
Client MAC Address	The MAC address of the wireless client (if applicable).
Client IP Address	The IP address of the wireless client (if applicable).
Interface	The interface number.

captive-portal client deauthenticate

M4250

M4350

This command deauthenticates a specific captive portal client. You can specify a captive portal configuration ID to indicate the captive portal configuration that the client is deauthenticating from. The optional *cp-id* variable is the captive portal ID, which ranges

from 1-10. If no value is entered, then the specified clients (or all clients) are deauthenticated from all captive portal configurations.

You can use the optional *macaddr* variable to specify the MAC address of the client to deauthenticate. If no value is specified, then all clients are deauthenticated from the specified captive portal configuration (or all configurations).

Format	<code>captive-portal client deauthenticate [cp-id] [macaddr]</code>
Mode	Privileged EXEC

Captive Portal Interface Commands

Use the commands in this section to view information about the interfaces on the switch that are associated with captive portals or that are capable of supporting a captive portal.

show captive-portal interface configuration status

M4250

M4350

This command displays the interface to configuration assignments for all captive portal configurations or a specific configuration. The optional *cp-id* variable is the captive portal ID, which ranges from 1-10.

Format	<code>show captive-portal interface configuration [cp-id] status</code>
Mode	Privileged EXEC

Term	Description
CP ID	Shows the captive portal ID the connected client is using.
CP Name	Shows the name of the captive portal the connected client is using.
Interface	Valid unit and port number separated by a forward slash.
Interface Description	Describes the interface.
Type	Shows the type of interface.

show captive-portal interface capability

M4250**M4350**

This command displays all the captive portal eligible interfaces or the interface capabilities for a specific captive portal interface.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show captive-portal interface capability [<i>unit/slot/port</i>]
Mode	Privileged EXEC
Field	Description
Interface	Valid unit and port number separated by a forward slash.
Interface Description	Describes the interface.
Type	Shows the type of interface.
If you specify a single interface, the following additional information displays:	
Session Timeout	Indicates whether or not this field is supported by the specified captive portal interface.
Idle Timeout	Indicates whether or not this field is supported by the specified captive portal interface.
Bytes Received Counter	Indicates whether or not this field is supported by the specified captive portal interface.
Bytes Transmitted Counter	Indicates whether or not this field is supported by the specified captive portal interface.
Packets Received Counter	Indicates whether or not this field is supported by the specified captive portal interface.
Packets Transmitted Counter	Indicates whether or not this field is supported by the specified captive portal interface.
Roaming	Indicates whether or not this field is supported by the specified captive portal interface.

Captive Portal Local User and User Group Commands

Use these commands to view and configure captive portal users in the local database.

user (Captive Portal Config)

M4250

M4350

This command is used to create a local user. The *user-id* variable is the user ID, which can be a number between 1 and 128. The *username* variable is the name of the user and can have up to 32 alphanumeric characters. The *password* variable is 8-64 characters. The *encrypted-password* variable is 128 hexadecimal characters.

Two ways exist to create a user: with the **user name** command or with the **user password** command. If you create the user with the **user name** command, you must assign the password with the **user password** command. If you create the user with the **user password** command, you can assign the name with the **user name** command at a later time.

You can also modify the password after you create a user by using the **user password** command with the user ID and a new password.

Format	<code>user user-id name username</code>
Mode	Captive Portal Config

Format	<code>user user-id password {password encrypted encrypted-password}</code>
Mode	Captive Portal Config

Command example:

The following example uses the name option to create the user.

```
(NETGEAR Switch) (Config-CP) #user 1 name testuser
```

Command example:

The following example uses the password option to create the user:

```
(NETGEAR Switch) (Config-CP) #user 1 password test1234
```

no user (Captive Portal Config)

This command deletes a user from the local user database. If the user has an existing session, it is disconnected. The *user-id* variable is the user ID, which can be a number between 1 and 128.

Format	<i>no user user-id</i>

Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch) (Config-CP) #no user 1
```

user name (Captive Portal Config)

M4250**M4350**

This command assigns a name to the user ID. This name is used at the client station for authentication. The *user-id* variable is the local user ID created with the **user** command and can be from 1 to 128 characters. The *username* variable is the name of the user and can have up to 32 alphanumeric characters.

Format	<i>user user-id name username</i>

Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch) (Config-CP) #user 1 name johnsmith
```

user password (Captive Portal Config)

M4250**M4350**

This command sets or modifies the password for the associated captive portal user. The *user-id* variable is the local user ID created with the user command and can be from 1 to 128 characters. The *password* variable is the user id's password and can have from 8 to 64 alphanumeric characters.

Format	<i>user user-id password password</i>

Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch)(Config-CP) #user 1 password
Enter Password (8 - 64 characters):
Re-enter password:
```

user password encrypted (Captive Portal Config)

M4250**M4350**

This command modifies the password for the associated captive portal user. The command accepts the password in an encrypted format. This command is used primarily by the **show running config** command process.

The *user-id* variable is the local user ID created with the user command. The *encrypted-pwd* variable is the password in encrypted format, which can be up to 128 hexadecimal characters.

Format	user <i>user-id</i> password encrypted <i>encrypted-password</i>
Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch)(Config-CP) #user 1 password encrypted 42 65 74 74 65 72 20 73 61 66 65
20 74 68 61 6e 20 73 6f 72 72 79
```

user session-timeout (Captive Portal Config)

M4250**M4350**

This command sets the session timeout value for the associated captive portal user. The *user-id* variable is the ID of a user configured in the local database, and is a number in the range of 1 to 128. The *timeout* variable is a number that represents the session time-out in from 0 to 86400 seconds. Enter 0 to indicate that the time-out is not enforced.

Default	0
Format	user <i>user-id</i> session-timeout <i>timeout</i>
Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch)(Config-CP) #user 1 session-timeout 86400
```


no user session-timeout (Captive Portal Config)

This command sets the session timeout value for the associated captive portal user to the default value. The *user-id* variable is the ID of a user configured in the local database, and is a number in the range of 1 to 128.

Format	no user <i>user-id</i> session-timeout

Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch) (Config-CP) #no user 1 session-timeout
```

user idle-timeout (Captive Portal Config)

M4250**M4350**

This command sets the session idle timeout value for the associated captive portal user. The *user-id* variable is the ID of a user configured in the local database, and is a number in the range of 1 to 128. The *timeout* variable is a number that represents the idle time-out from 0 to 900 seconds. Use 0 to indicate that the time-out is not enforced.

Default	0

Format	user <i>user-id</i> idle-timeout <i>timeout</i>

Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch) (Config-CP) #user 1 idle-timeout 600
```

no user idle-timeout

This command sets the session idle timeout value for the associated captive portal user to the default value. The *user-id* variable is the ID of a user configured in the local database, and is a number in the range of 1 to 128.

Format	no user <i>user-id</i> idle-timeout

Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch) (Config-CP) #no user 1 idle-timeout
```

user max-bandwidth-up (Captive Portal Config)

M4250**M4350**

This command is used to configure the bandwidth from 0 to 536870911 bytes per second (bps, with the *bps* variable) at which the client can send data into the network. 0 denotes using the default value configured for the captive portal. The *user-id* variable is the ID of a user configured in the local database, and is a number in the range of 1 to 128.

Default	0
Format	user user-id max-bandwidth-up bps
Mode	Captive Portal Config

Parameter	Description
user-id	User ID from 1 to 128 characters.
bps	Client transmit rate in bytes per second (bps). 0 denotes unlimited bandwidth.

no user max-bandwidth-up (Captive Portal Config)

Use this command to set to the default the bandwidth at which the client can send data into the network. The *user-id* variable is the ID of a user configured in the local database, and is a number in the range of 1 to 128.

Format	no user user-id max-bandwidth-up
Mode	Captive Portal Config

user max-bandwidth-down (Captive Portal Config)

M4250**M4350**

This command is used configure the bandwidth from 0 to 536870911 bytes per second (bps, with the variable) at which the client can receive data from the network. 0 denotes using the default value configured for the captive portal. The *user-id* variable is the ID of a user configured in the local database, and is a number in the range of 1 to 128.

Default	0
Format	user user-id max-bandwidth-down bps
Mode	Captive Portal Config

Parameter	Description
user-id	User ID from 1 to 128 characters.
bps	Client receive rate in bps. 0 denotes unlimited bandwidth.

no user max-bandwidth down (Captive Portal Config)

Use this command to set to the default value the bandwidth at which the client can receive data from the network. The *user-id* variable is the ID of a user configured in the local database, and is a number in the range of 1 to 128.

Format	no user <i>user-id</i> max-bandwidth-down
Mode	Captive Portal Config

user max-input-octets (Captive Portal Config)

M4250

M4350

This command is used to limit the number of octets from 0 to 4294967295 bytes that the user is allowed to transmit. After this limit has been reached, the user will be disconnected. 0 octets denote unlimited transmission. The *user-id* variable is the ID of a user configured in the local database, and is a number in the range of 1 to 128.

Default	0
Format	user <i>user-id</i> max-input-octets <i>octets</i>
Mode	Captive Portal Config

Parameter	Description
user-id	User ID from 1 to 128 characters.
octets	Number of bytes.

no user max-input-octets (Captive Portal Config)

Use this command to set to the default the number of octets in bytes that the user is allowed to transmit. The *user-id* variable is the ID of a user configured in the local database, and is a number in the range of 1 to 128.

Format	no user <i>user-id</i> max-input-octets
Mode	Captive Portal Config

user max-output-octets (Captive Portal Config)

M4250**M4350**

This command is used to limit the number of octets from 0 to 4294967295 bytes that the user is allowed to receive. After this limit has been reached, the user will be disconnected. 0 octets denote unlimited transmission. The *user-id* variable is the ID of a user configured in the local database, and is a number in the range of 1 to 128.

Default	0
Format	<i>user user-id max-output-octets octets</i>
Mode	Captive Portal Config

Parameter	Description
user-id	User ID from 1 to 128 characters.
octets	Number of bytes.

no user max-output-octets (Captive Portal Config)

Use this command to set to the default the number of octets in bytes that the user is allowed to receive. The *user-id* variable is the ID of a user configured in the local database, and is a number in the range of 1 to 128.

Format	<i>no user user-id max-output-octets</i>
Mode	Captive Portal Config

user max-total-octets (Captive Portal Config)

M4250**M4350**

This command is used to limit the number of octets from 0 to 4294967295 bytes that the user is allowed to transmit and receive. The maximum number of octets is the sum of octets transmitted and received. After this limit has been reached, the user will be disconnected. 0 octets denote unlimited transmission. The *user-id* variable is the ID of a user configured in the local database, and is a number in the range of 1 to 128.

Default	0
Format	<i>user user-id max-total-octets octets</i>
Mode	Captive Portal Config

Parameter	Description
user-id	User ID from 1 to 128 characters.
octets	Number of bytes.

no user max-total-octets (Captive Portal Config)

Use this command to set to the default the number of octets in bytes that the user is allowed to transmit and receive. The *user-id* variable is the ID of a user configured in the local database, and is a number in the range of 1 to 128.

Format	no user <i>user-id</i> max-total-octets
Mode	Captive Portal Config

user group (Captive Portal Config)

M4250

M4350

Use this command to create a user group. The *group-id* variable is a number in the range of 1–10.

Format	user group <i>group-id</i>
Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch) (Config-CP) #user group 1
```

no user group (Captive Portal Config)

Use this command to delete a user group. The *group-id* variable is a number in the range of 1–10.

Format	no user group <i>group-id</i>
Mode	Captive Portal Config

user group name (Captive Portal Config)

M4250**M4350**

Use this command to configure a group name. The *group-id* variable is a number in the range of 1–10. The *name* variable can be up to 32 alphanumeric characters.

Format	<i>user group group-id name name</i>
Mode	Captive Portal Config

user {user-id} group (Captive Portal Config)

M4250**M4350**

This command assigns or modifies a specific captive portal user to a captive portal group. The *user-id* variable is the user ID, which is a number in the range of 1 to 128). The *group-id* variable is the group ID in the range of 1 to 10.

Format	<i>user user-id group group-id</i>
Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch) (Config-CP) #user 1 group 1
```

user group moveusers (Captive Portal Config)

M4250**M4350**

This command moves existing users from one user group to another. Note that the destination group must already exist before a move can be successful. The *group-id* and *destination-group-id* variables are each a number in the range of 1-10.

Format	<i>user group group-id moveusers destination-group-id</i>
Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch) (Config-CP) #user group 2 moveusers 3
```

show captive-portal user

M4250**M4350**

This command displays all configured users or a specific user in the captive portal local user database. Enter the optional user ID to view information about the specified user. The optional *user-id* variable is the ID of a user configured in the local database, and is a number in the range of 1 to 128. Enter the **group** keyword or the group keyword and *group-id* variable to view the user information organized by groups.

Format	show captive-portal user [<i>user-id</i>] [group [<i>group-id</i>]]
Mode	Privileged EXEC
Field	Description
User ID	Displays the ID of the user.
User Name	Displays the user name.
Session Timeout	Displays the number of seconds the user can remain in a session before being disconnected from the Captive Portal.
Idle Timeout	Displays the number of seconds the user can remain idle before being disconnected from the Captive Portal.
Group ID	Displays the group identifier for the group to which the user belongs.
When you include the [<i>user-id</i>] variable, the following information also displays:	
Password Configured	Indicates whether a password has been configured for the user.
Max Bandwidth Up (bps)	The maximum rate in bytes per second (bps) at which a client can send data into the network.
Max Bandwidth Down (bps)	The maximum rate in bps at which a client can receive data from the network.
Max Bandwidth Input Octets (bytes)	The maximum number of octets the user is allowed to transmit.
Max Bandwidth Output Octets (bytes)	The maximum number of octets the user is allowed to receive.
Max Bandwidth Total Octets (bytes)	The maximum number of octets the user is allowed to transfer, i.e., the sum of octets transmitted and received.

clear captive-portal users

M4250

M4350

This command deletes all captive portal user entries.

Format	clear captive-portal users

Mode	Privileged EXEC

10

IPv6 Commands

This chapter describes the IPv6 commands. The chapter contains the following sections:

- [Loopback Interface Commands](#)
- [IPv6 Routing Commands](#)
- [IPv6 Policy-Based Routing Commands](#)
- [OSPFv3 Commands](#)
- [DHCPv6 Commands](#)
- [DHCPv6 Snooping Configuration Commands](#)

The commands in this chapter are in one of three functional groups:

- **Show commands.** Display switch settings, statistics, and other information.
- **Configuration commands.** Configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- **Clear commands.** Clear some or all of the settings to factory defaults.

Note: For information about IPv6 management commands, see [IPv6 Management Commands](#).

Loopback Interface Commands

The commands in this section describe how to create, delete, and manage loopback interfaces. A loopback interface is always expected to be up. This interface can provide the source address for sent packets and can receive both local and remote packets. The loopback interface is typically used by routing protocols.

To assign an IP address to the loopback interface, see [ip address on page 915](#). To assign an IPv6 address to the loopback interface, see [ipv6 address on page 1143](#).

interface loopback

M4250

M4350

Use this command to enter the Interface Config mode for a loopback interface. The range of the loopback ID is from 0 to 63.

Format	<code>interface loopback <i>loopback-id</i></code>
Mode	Global Config

no interface loopback

This command removes the loopback interface and associated configuration parameters for the specified loopback interface.

Format	<code>no interface loopback <i>loopback-id</i></code>
Mode	Global Config

show interface loopback

M4250

M4350

This command displays information about configured loopback interfaces.

Format	<code>show interface loopback [<i>loopback-id</i>]</code>
Mode	Privileged EXEC

If you do not specify a loopback ID, the following information appears for each loopback interface on the system.

Term	Definition
Loopback ID	The loopback ID associated with the rest of the information in the row.
Interface	The interface name.
IP Address	The IPv4 address of the interface.

If you specify a loopback ID, the following information appears.

Term	Definition
Interface Link Status	Shows whether the link is up or down.
IP Address	The IPv4 address of the interface.
MTU size	The maximum transmission size for packets on this interface, in bytes.

IPv6 Routing Commands

This section describes the IPv6 commands you use to configure IPv6 on the system and on the interfaces. This section also describes IPv6 management commands and show commands.

ipv6 hop-limit

M4250

M4350

This command defines the unicast hop count used in ipv6 packets originated by the node. The value is also included in router advertisements. Valid values for *hops* are 1-255 inclusive. The default “not configured” means that a value of zero is sent in router advertisements and a value of 64 is sent in packets originated by the node. Note that this is not the same as configuring a value of 64.

Default	not configured
Format	<code>ipv6 hop-limit hops</code>
Mode	Global Config

no ipv6 hop-limit

This command returns the unicast hop count to the default.

Format	no ipv6 hop-limit
Mode	Global Config

ipv6 unicast-routing

M4250

M4350

Use this command to enable the forwarding of IPv6 unicast datagrams.

Default	disabled
Format	ipv6 unicast-routing
Mode	Global Config

no ipv6 unicast-routing

Use this command to disable the forwarding of IPv6 unicast datagrams.

Format	no ipv6 unicast-routing
Mode	Global Config

ipv6 enable

M4250

M4350

Use this command to enable IPv6 routing on an interface or range of interfaces, including loopback interfaces, that have not been configured with an explicit IPv6 address. When you use this command, the interface is automatically configured with a link-local address. You do not need to use this command if you configured an IPv6 global address on the interface.

Default	disabled
Format	ipv6 enable
Mode	Interface Config

no ipv6 enable

Use this command to disable IPv6 routing on an interface.

Format	no ipv6 enable

Mode	Interface Config

ipv6 address

M4250

M4350

Use this command to configure an IPv6 address on an interface or range of interfaces, including loopback interfaces, and to enable IPv6 processing on the interfaces. You can assign multiple globally reachable addresses to an interface by using this command. You do not need to assign a link-local address by using this command since one is automatically created. The *prefix* field consists of the bits of the address to be configured. The *prefix_length* parameter designates how many of the high-order contiguous bits of the address make up the prefix.

You can express IPv6 addresses in eight blocks. Also of note is that instead of a period, a colon now separates each block. For simplification, leading zeros of each 16 bit block can be omitted. One sequence of 16 bit blocks containing only zeros can be replaced with a double colon "::", but not more than one at a time (otherwise it is no longer a unique representation).

- Dropping zeros: 3ffe:ffff:100:f101:0:0:0:1 becomes 3ffe:ffff:100:f101::1
- Local host: 0000:0000:0000:0000:0000:0000:0000:0001 becomes ::1
- Any host: 0000:0000:0000:0000:0000:0000:0000:0000 becomes ::

The hexadecimal letters in the IPv6 addresses are not case-sensitive. An example of an IPv6 prefix and prefix length is 3ffe:1::1234/64.

The optional **eui-64** keyword designates that IPv6 processing on the interface is enabled using an EUI-64 interface ID in the low order 64 bits of the address. If you use this option, the value of *prefix_length* must be 64 bits. The optional **link-local** keyword designates that IPv6 processing on the interface is enabled using the link-local address.

Format	ipv6 address <i>prefix/prefix_length</i> [eui64 link-local]

Mode	Interface Config

no ipv6 address

Use this command to remove all IPv6 addresses on an interface or specified IPv6 address. The *prefix* parameter consists of the bits of the address to be configured. The *prefix_length* parameter designates how many of the high-order contiguous bits of the address comprise the prefix.

The optional **eui-64** keyword designates that IPv6 processing on the interface is enabled using an EUI-64 interface ID in the low order 64 bits of the address. If you use this option, the

value of *prefix_length* must be 64 bits. The optional **link-local** keyword designates that IPv6 processing on the interface is enabled using the link-local address.

If you do not enter any parameters, the command deletes all the IPv6 addresses on an interface.

Format	<code>no ipv6 address [prefix/prefix_length [eui64 link-local]]</code>

Mode	Interface Config

ipv6 address autoconfig

M4250

M4350

Use this command to allow an in-band interface to acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of Router Advertisement messages.

Default	disabled

Format	<code>ipv6 address autoconfig</code>

Mode	Interface Config

no ipv6 address autoconfig

This command the IPv6 autoconfiguration status on an interface to the default value.

Format	<code>no ipv6 address autoconfig</code>

Mode	Interface Config

ipv6 address dhcp

M4250

M4350

This command enables the DHCPv6 client on an in-band interface so that it can acquire network information, such as the IPv6 address, from a network DHCP server.

Default	disabled

Format	<code>ipv6 address dhcp</code>

Mode	Interface Config

no ipv6 address dhcp

This command releases a leased address and disables DHCPv6 on an interface.

Format	no ipv6 address dhcp

Mode	Interface Config

ipv6 route (M4250 series switch)

M4250

Use this command to configure an IPv6 static route. The *ipv6-prefix* is the IPv6 network that is the destination of the static route. The *prefix-length* is the length of the IPv6 prefix—a decimal value (usually 0-64) that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the *prefix-length*. The *next-hop-address* is the IPv6 address of the next hop that can be used to reach the specified network. Specifying **Null0** as nexthop parameter adds a static reject route.

The **preference** parameter is a value that the switch uses to compare this route with routes from other route sources that have the same destination. The range for *preference* is 1–255, and the default value is 1.

The **track** parameter is a value that the switch uses for association with a track object. The range for *track-number* is 1–128.

You can specify a *slot/port* or *vlan-id* interface to identify direct static routes from point-to-point and broadcast interfaces.

The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

The interface must be specified when using a link-local address as the next hop. A route with a preference of 255 cannot be used to forward traffic.

Default	disabled

Format	ipv6 route <i>ipv6-prefix/prefix-length</i> { <i>next-hop-address</i> Null0 interface { <i>slot/port</i> vlan <i>vlan-id</i> } <i>next-hop-address</i> } [<i>preference</i>] [track <i>track-number</i>]

Mode	Global Config

no ipv6 route (M4250 series switch)

Use this command to delete an IPv6 static route. Use the command without the optional parameters to delete all static routes to the specified destination. Use the *preference* parameter to revert the preference of a route to the default preference.

Format	<code>no ipv6 route ipv6-prefix/prefix-length [{next-hop-address Null0 interface {slot/port vlan vlan-id} next-hop-address} [preference] [track track-number]]</code>

Mode	Global Config

ipv6 route (M4350 series switch)

M4350

Use this command to configure an IPv6 static route. The *ipv6-prefix* is the IPv6 network that is the destination of the static route. The *prefix-length* is the length of the IPv6 prefix—a decimal value (usually 0-64) that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the *prefix-length*. The *next-hop-address* is the IPv6 address of the next hop that can be used to reach the specified network. Specifying **Null0** as nexthop parameter adds a static reject route.

The **preference** parameter is a value that the switch uses to compare this route with routes from other route sources that have the same destination. The range for *preference* is 1–255, and the default value is 1.

The **track** parameter is a value that the switch uses for association with a track object. The range for *track-number* is 1–128.

You can specify a *unit/slot/port* or *vlan-id* interface to identify direct static routes from point-to-point and broadcast interfaces.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

The interface must be specified when using a link-local address as the next hop. A route with a preference of 255 cannot be used to forward traffic.

Default	disabled
Format	<code>ipv6 route ipv6-prefix/prefix-length {next-hop-address Null0 interface {unit/slot/port vlan vlan-id} next-hop-address} [preference] [track track-number]</code>
Mode	Global Config

no ipv6 route (M4350 series switch)

Use this command to delete an IPv6 static route. Use the command without the optional parameters to delete all static routes to the specified destination. Use the *preference* parameter to revert the preference of a route to the default preference.

Format	<code>no ipv6 route ipv6-prefix/prefix-length [{next-hop-address Null0 interface {unit/slot/port vlan vlan-id} next-hop-address} [preference] [track track-number]]</code>

Mode	Global Config

ipv6 route distance

M4250

M4350

This command sets the default distance (preference) for IPv6 static routes. Lower route distance values are preferred when determining the best route. The **ipv6 route distance** command lets you optionally set the distance (preference) of an individual static route. The default distance is used when no distance is specified in this command. The *preference* can be a number in the range 1–255.

Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after entering the **ipv6 route distance** command.

Default	1

Format	<code>ipv6 route distance preference</code>

Mode	Global Config

no ipv6 route distance

This command resets the default static route preference value in the router to the original default preference. Lower route preference values are preferred when determining the best route.

Format	<code>no ipv6 route distance</code>

Mode	Global Config

ipv6 route net-prototype

M4250

M4350

This command adds net prototype IPv6 routes to the hardware.

Use the *prefix/prefix-length* argument to specify the The destination network and mask for the route.

Use the *next-hop-address* argument to specify the next-hop IP address, which must belong to an active routing interface but it does not need to be resolved. The routes are added starting from the specified prefix and prefix-length.

Use the *num-routes* argument to specify the number of routes that you want to add to the hardware.

Format	<code>ipv6 route net-prototype <i>prefix/prefix-length</i> <i>next-hop-address</i> <i>num-routes</i></code>
Mode	Global Config

no ipv6 route net-prototype

This command removes all net prototype IPv6 routes from the hardware.

Format	<code>no ipv6 route net-prototype</code>
Mode	Global Config

ipv6 mtu (M4250 series switch)

M4250

This command sets the maximum transmission unit (MTU) size, in bytes, of IPv6 packets on an interface or range of interfaces. This command replaces the default or link MTU with a new MTU value. The *size* variable is a number in the range from 1280 to the maximum MTU that the interface is capable of minus 18. For an M4250 series switch, the range is from 1280–12270.

Default	0 or link speed (MTU value (1500))
Format	<code>ipv6 mtu <i>size</i></code>
Mode	Interface Config

no ipv6 mtu (M4250 series switch)

This command resets maximum transmission unit value to default value.

Format	<code>no ipv6 mtu</code>
Mode	Interface Config

ipv6 mtu (M4350 series switch)

M4350

This command sets the maximum transmission unit (MTU) size, in bytes, of IPv6 packets on an interface or range of interfaces. This command replaces the default or link MTU with a new MTU value. The *size* variable is a number in the range from 1280 to the maximum MTU that the interface is capable of minus 18. For an M4350 series switch, the range is from 1280–12266.

Default	0 or link speed (MTU value (1500))
Format	ipv6 mtu <i>size</i>
Mode	Interface Config

no ipv6 mtu (M4350 series switch)

This command resets maximum transmission unit value to default value.

Format	no ipv6 mtu
Mode	Interface Config

ipv6 nd dad attempts

M4250**M4350**

This command sets the number of duplicate address detection probes transmitted on an interface or range of interfaces. The purpose of these transmissions is neighbor discovery (ND). Duplicate address detection verifies that an IPv6 address on an interface is unique. The *number* variable is a number in the range 0–600.

Default	1
Format	ipv6 nd dad attempts <i>number</i>
Mode	Interface Config

no ipv6 nd dad attempts

This command resets to number of duplicate address detection value to default value.

Format	no ipv6 nd dad attempts
Mode	Interface Config

ipv6 nd managed-config-flag

M4250

M4350

This command sets the managed address configuration flag in router advertisements on the interface or range of interfaces. The purpose of these advertisement is neighbor discovery (ND). When the value is true, end nodes use DHCPv6. When the value is false, end nodes automatically configure addresses.

Default	false
Format	ipv6 nd managed-config-flag
Mode	Interface Config

no ipv6 nd managed-config-flag

This command resets the “managed address configuration” flag in router advertisements to the default value.

Format	no ipv6 nd managed-config-flag
Mode	Interface Config

ipv6 nd mtu (M4250 series switch)

M4250

This command sets the MTU value for IPv6 router advertisements on an interface. The purpose of these advertisement is neighbor discovery (ND). The *size* argument is a number in the range from 1280 to the maximum MTU that the interface is capable of minus 18. For an M4250 series switch, the range is from 1280–12270.

Default	0
Format	ipv6 nd mtu <i>size</i>
Mode	Interface Config

no ipv6 nd mtu (M4250 series switch)

This command resets the MTU value for IPv6 router advertisements on an interface to 0.

Format	no ipv6 nd mtu
Mode	Interface Config

ipv6 nd mtu (M4350 series switch)

M4350

This command sets the MTU value for IPv6 router advertisements on an interface. The purpose of these advertisement is neighbor discovery (ND). The *size* argument is a number in the range from 1280 to the maximum MTU that the interface is capable of minus 18. For an M4350 series switch, the range is from 1280–12266.

Default	0
Format	ipv6 nd mtu <i>size</i>
Mode	Interface Config

no ipv6 nd mtu (M4350 series switch)

This command resets the MTU value for IPv6 router advertisements on an interface to 0.

Format	no ipv6 nd mtu
Mode	Interface Config

ipv6 nd ns-interval

M4250**M4350**

This command sets the interval between router advertisements for advertised neighbor solicitations, in milliseconds. An advertised value of 0 means the interval is unspecified. This command can configure a single interface or a range of interfaces. The *milliseconds* variable is a period in milliseconds in the range of 1000–4294967295.

Default	0
Format	ipv6 nd ns-interval { <i>milliseconds</i> 0}
Mode	Interface Config

no ipv6 nd ns-interval

This command resets the neighbor solicit retransmission interval of the specified interface to the default value.

Format	no ipv6 nd ns-interval
Mode	Interface Config

ipv6 nd other-config-flag

M4250

M4350

This command sets the “other stateful configuration” flag in router advertisements sent from the interface. The purpose of these advertisement is neighbor discovery (ND).

Default	false
Format	ipv6 nd other-config-flag
Mode	Interface Config

no ipv6 nd other-config-flag

This command resets the “other stateful configuration” flag back to its default value in router advertisements sent from the interface.

Format	no ipv6 nd other-config-flag
Mode	Interface Config

ipv6 nd ra-interval

M4250

M4350

This command sets the transmission interval between router advertisements on the interface or range of interfaces. The purpose of these advertisement is neighbor discovery (ND). The *seconds* variable is a number in the range 4–1800 seconds.

Default	600
Format	ipv6 nd ra-interval-max <i>seconds</i>
Mode	Interface Config

no ipv6 nd ra-interval

This command sets router advertisement interval to the default.

Format	no ipv6 nd ra-interval-max
Mode	Interface Config

ipv6 nd ra-lifetime

M4250

M4350

This command sets the value, in seconds, that is placed in the Router Lifetime field of the router advertisements sent from the interface or range of interfaces. The purpose of these advertisement is neighbor discovery (ND). The *lifetime* variable can be zero, or it must be an integer between the value of the router advertisement transmission interval and 9000. A value of zero means this router is not to be used as the default router.

Default	1800
Format	ipv6 nd ra-lifetime <i>lifetime</i>
Mode	Interface Config

no ipv6 nd ra-lifetime

This command resets router lifetime to the default value.

Format	no ipv6 nd ra-lifetime
Mode	Interface Config

ipv6 nd raguard attach-policy

M4250

M4350

This command enables the IPv6 RA guard host mode on the configured interface. All router advertisement (RAs) and router redirect packets for neighbor discovery (ND) that are received on this interface are dropped.

Format	ipv6 nd raguard attach-policy
Mode	Interface Config

no ipv6 nd raguard attach-policy

This command disables the IPv6 RA guard host mode on the configured interface.

Format	no ipv6 nd raguard attach-policy
Mode	Interface Config

ipv6 nd ra hop-limit unspecified

M4250

M4350

This command configures the switch to send router advertisements on an interface with an unspecified (0) Current Hop Limit value. The purpose of these advertisement is neighbor discovery (ND), and they inform the hosts on that link to ignore the Hop Limit from the switch.

Default	Disable
Format	<code>ipv6 nd ra hop-limit unspecified</code>
Mode	Interface Config

no ipv6 nd ra hop-limit unspecified

This command configures the router to send Router Advertisements on an interface with the global configured Hop Limit value.

Format	<code>no ipv6 nd ra hop-limit unspecified</code>
Mode	Interface Config

ipv6 nd reachable-time

M4250

M4350

This command sets the router advertisement time to consider a neighbor reachable after neighbor discovery (ND) confirmation. Reachable time is specified in milliseconds in a range from 0–4294967295 milliseconds. A value of zero means that the time is unspecified by the switch.

Default	0
Format	<code>ipv6 nd reachable-time <i>milliseconds</i></code>
Mode	Interface Config

no ipv6 nd reachable-time

This command means reachable time is unspecified for the switch.

Format	<code>no ipv6 nd reachable-time</code>
Mode	Interface Config

ipv6 nd router-preference

M4250

M4350

Use this command to configure default router preferences that the interface advertises in router advertisement messages. The purpose of these advertisement is neighbor discovery (ND).

Default	medium
Format	ipv6 nd router-preference {low medium high}
Mode	Interface Config

no ipv6 nd router-preference

This command resets the router preference advertised by the interface to the default value.

Format	no ipv6 nd router-preference
Mode	Interface Config

ipv6 nd suppress-ra

M4250

M4350

This command suppresses router advertisement transmission on an interface or range of interfaces. The purpose of these advertisement is neighbor discovery (ND).

Default	disabled
Format	ipv6 nd suppress-ra
Mode	Interface Config

no ipv6 nd suppress-ra

This command enables router transmission on an interface.

Format	no ipv6 nd suppress-ra
Mode	Interface Config

ipv6 nd prefix

M4250

M4350

Use the **ipv6 nd prefix** command to configure parameters associated with prefixes the router advertises in its router advertisements. The purpose of these advertisement is neighbor discovery (ND). The first optional parameter is the valid lifetime of the switch, in seconds in the range of 0–4294967295 seconds. You can specify a value or indicate that the lifetime value is infinite. The second optional parameter is the preferred lifetime of the switch in seconds in the range of 0–4294967295 seconds.

This command can be used to configure a single interface or a range of interfaces.

The router advertises its global IPv6 prefixes in its router advertisements (RAs). An RA only includes the prefixes of the IPv6 addresses configured on the interface where the RA is transmitted. Addresses are configured using the **ipv6 address** interface configuration command. Each prefix advertisement includes information about the prefix, such as its lifetime values and whether hosts should use the prefix for on-link determination or address auto-configuration. Use the **ipv6 nd prefix** command to configure these values.

The **ipv6 nd prefix** command allows you to preconfigure RA prefix values before you configure the associated interface address. In order for the prefix to be included in RAs, you must configure an address that matches the prefix using the **ipv6 address** command. Prefixes specified using **ipv6 nd prefix** without associated interface address will not be included in RAs and will not be committed to the device configuration.

Default	valid-lifetime—2592000 preferred-lifetime— 604800 autoconfig—enabled on-link—enabled
Format	<code>ipv6 nd prefix <i>prefix/prefix_length</i> [{<i>seconds</i> infinite} {<i>seconds</i> infinite}] [no-autoconfig] [off-link]</code>
Mode	Interface Config

no ipv6 nd prefix

This command sets prefix configuration to default values.

Format	<code>no ipv6 nd prefix <i>prefix/prefix_length</i></code>
Mode	Interface Config

ipv6 neighbor

M4250

M4350

This command configures a static IPv6 neighbor with a specific IPv6 address and MAC address on a routing or host interface.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

Format	<code>ipv6 neighbor ipv6address {unit/slot/port vlan vlan-id} macaddr</code>
Mode	Global Config
Parameter	Definition
ipv6address	The IPv6 address of the neighbor.
unit/slot/port	The interface.
vlan-id	The VLAN for the interface.
macaddr	The MAC address for the neighbor.

no ipv6 neighbor

This command removes a static IPv6 neighbor for a specific IPv6 address on a routing or host interface.

Format	<code>no ipv6 neighbor ipv6address {unit/slot/port vlan vlan-id}</code>
Mode	Global Config

ipv6 neighbors dynamicrenew

M4250

M4350

This command automatically renews the IPv6 neighbor entries. The command enables the periodic neighbor unreachability detection (NUD) on the existing IPv6 neighbor entries based on the activity of the entries in the hardware. Every 40 seconds, a set of 300 entries are triggered for NUD, irrespective of their usage in the hardware.

Default	Disabled
Format	ipv6 neighbors dynamicrenew
Mode	Global Config

no ipv6 neighbors dynamicrenew

This command disables automatic renewing of IPv6 neighbor entries, causing only those entries that are actively used in the hardware to be triggered for NUD at the end of a stale time-out of 1200 seconds.

Format	no ipv6 neighbors dynamicrenew
Mode	Global Config

ipv6 nud

M4250

M4350

This command configures a Neighbor Unreachability Detection (NUD) option. NUD verifies that communication with a neighbor exists.

Format	ipv6 nud {backoff-multiple max-multicast-solicits max-unicast-solicits}
Mode	Global Config

Term	Definition
backoff-multiple	Sets the exponential backoff multiple to calculate time outs in NS transmissions during NUD. The value ranges from 1 to 5. 1 is the default. The next timeout value is limited to a maximum value of 60 seconds if the value with exponential backoff calculation is greater than 60 seconds.
max-multicast-solicits	Sets the maximum number of multicast solicits sent during Neighbor Unreachability Detection. The value ranges from 3 to 255. 3 is the default.
max-unicast-solicits	Sets the maximum number of unicast solicits sent during Neighbor Unreachability Detection. The value ranges from 3 to 10. 3 is the default.

no ipv6 nud

This command disables the Neighbor Unreachability Detection (NUD) option.

Format	no ipv6 nud {backoff-multiple max-multicast-solicits max-unicast-solicits}
Mode	Global Config

ipv6 unreachable

M4250

M4350

Use this command to enable the generation of ICMPv6 Destination Unreachable messages on the interface or range of interfaces. By default, the generation of ICMPv6 Destination Unreachable messages is enabled.

Default	enable
Format	ipv6 unreachable
Mode	Interface Config

no ipv6 unreachable

Use this command to prevent the generation of ICMPv6 Destination Unreachable messages.

Format	no ipv6 unreachable
Mode	Interface Config

ipv6 unresolved-traffic

M4250

M4350

Use this command to control the rate at which IPv6 data packets come into the CPU. By default, rate limiting is disabled. When enabled, the rate, expressed by the *seconds* variable, can range from 5 to 1024 packets per second.

Default	enable
Format	ipv6 unresolved-traffic rate-limit <i>seconds</i>
Mode	Global Config

no ipv6 unresolved-traffic

Use this command to disable the rate limiting.

Format	no ipv6 unresolved-traffic rate-limit
Mode	Global Config

ipv6 icmp error-interval

M4250

M4350

Use this command to limit the rate at which ICMPv6 error messages are sent. The rate limit is configured as a token bucket, with two configurable parameters, *burst-size* and *burst-interval*.

The *burst-interval* specifies how often the token bucket is initialized with *burst-size* tokens. *burst-interval* is from 0 to 2147483647 milliseconds (msec).

The *burst-size* is the number of ICMPv6 error messages that can be sent during one *burst-interval*. The range is from 1 to 200 messages.

To disable ICMP rate limiting, set the *burst-interval* argument to zero (0).

Default	<i>burst-interval</i> of 1000 msec. <i>burst-size</i> of 100 messages
Format	ipv6 icmp error-interval <i>burst-interval</i> [<i>burst-size</i>]
Mode	Global Config

no ipv6 icmp error-interval

Use this command to return the burst interval and burst size to their default values.

Format	no ipv6 icmp error-interval
Mode	Global Config

show ipv6 brief

M4250

M4350

Use this command to display the IPv6 status of the forwarding mode and IPv6 unicast routing mode.

Format	show ipv6 brief
Mode	Privileged EXEC

Term	Definition
IPv6 Forwarding Mode	Shows whether the IPv6 forwarding mode is enabled.
IPv6 Unicast Routing Mode	Shows whether the IPv6 unicast routing mode is enabled.
IPv6 Hop Limit	Shows the unicast hop count used in IPv6 packets originated by the node. For more information, see ipv6 hop-limit on page 1141.

Term	Definition
ICMPv6 Rate Limit Error Interval	Shows how often the token bucket is initialized with burst-size tokens. For more information, see ipv6 icmp error-interval on page 1160 .
ICMPv6 Rate Limit Burst Size	Shows the number of ICMPv6 error messages that can be sent during one <i>burst-interval</i> . For more information, see ipv6 icmp error-interval on page 1160 .
Maximum Routes	Shows the maximum IPv6 route table size.
IPv6 Unresolved Data Rate Limit	Shows the rate in packets-per-second for the number of IPv6 data packets trapped to CPU when the packet fails to be forwarded in the hardware due to unresolved hardware address of the destined IPv6 node.
IPv6 Neighbors Dynamic Renew	Shows the dynamic renewal mode for the periodic NUD (neighbor unreachability detection) run on the existing IPv6 neighbor entries based on the activity of the entries in the hardware.
IPv6 NUD Maximum Unicast Solicits	Shows the maximum number of unicast Neighbor Solicitations sent during NUD (neighbor unreachability detection) before switching to multicast Neighbor Solicitations.
IPv6 NUD Maximum Multicast Solicits	Shows the maximum number of multicast Neighbor Solicitations sent during NUD (neighbor unreachability detection) when in UNREACHABLE state.
IPv6 NUD Exponential Backoff Multiple	Shows the exponential backoff multiple to be used in the calculation of the next timeout value for Neighbor Solicitation transmission during NUD (neighbor unreachability detection) following the exponential backoff algorithm.

Command example:

```
(NETGEAR Switch) #show ipv6 brief
```

```
IPv6 Unicast Routing Mode..... Disable
IPv6 Hop Limit..... 0
ICMPv6 Rate Limit Error Interval..... 1000 msec
ICMPv6 Rate Limit Burst Size..... 100 messages
Maximum Routes..... 4096

IPv6 Unresolved Data Rate Limit..... 1024 pps
IPv6 Neighbors Dynamic Renew..... Disable
IPv6 NUD Maximum Unicast Solicits..... 3
IPv6 NUD Maximum Multicast Solicits..... 3
IPv6 NUD Exponential Backoff Multiple..... 1
```

show ipv6 interface (M4250 series switch)

M4250

Use this command to show the usability status of IPv6 interfaces and whether ICMPv6 Destination Unreachable messages may be sent.

The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

The **loopback** keyword with the *number* variable specifies the loopback interface directly and is a number in the range 0–7.

Format	<code>show ipv6 interface [brief slot/port vlan vlan-id loopback number]</code>
Mode	Privileged EXEC

If you use the **brief** parameter, the following information displays for all configured IPv6 interfaces.

Term	Definition
Interface	The interface in <i>slot/port</i> format.
IPv6 Operational Mode	Shows whether the mode is enabled or disabled.
IPv6 Address/Length	Shows the IPv6 address and length on interfaces with IPv6 enabled.
Method	Indicates how each IP address was assigned. The field contains one of the following values: - DHCP. The address is leased from a DHCP server. - Manual. The address is manually configured. Global addresses with no annotation are assumed to be manually configured.

If you specify an interface, the following information also displays.

Term	Definition
Routing Mode	Shows whether IPv6 routing is enabled or disabled.
IPv6 Enable Mode	Shows whether IPv6 is enabled on the interface.
Administrative Mode	Shows whether the interface administrative mode is enabled or disabled.
Bandwidth	Shows bandwidth of the interface.
Interface Maximum Transmission Unit	The MTU size, in bytes.
Router Duplicate Address Detection Transmits	The number of consecutive duplicate address detection probes to transmit.
Address Autoconfigure Mode	Shows whether the autoconfigure mode is enabled or disabled.

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Address DHCP Mode	Shows whether the DHCPv6 client is enabled on the interface.
IPv6 Hop Limit Unspecified	Indicates if the router is configured on this interface to send Router Advertisements with unspecified (0) as the Current Hop Limit value.
Router Advertisement NS Interval	The interval, in milliseconds, between router advertisements for advertised neighbor solicitations.
Router Advertisement Lifetime	Shows the router lifetime value of the interface in router advertisements.
Router Advertisement Reachable Time	The amount of time, in milliseconds, to consider a neighbor reachable after neighbor discovery confirmation.
Router Advertisement Interval	The frequency, in seconds, that router advertisements are sent.
Router Advertisement Managed Config Flag	Shows whether the managed configuration flag is set (enabled) for router advertisements on this interface.
Router Advertisement Other Config Flag	Shows whether the other configuration flag is set (enabled) for router advertisements on this interface.
Router Advertisement Router Preference	Shows the router preference.
Router Advertisement Suppress Flag	Shows whether router advertisements are suppressed (enabled) or sent (disabled).
IPv6 Destination Unreachables	Shows whether ICMPv6 Destination Unreachable messages may be sent (enabled) or not (disabled). For more information, see ipv6 unreachable on page 1159 .
ICMPv6 Redirect	Specifies if ICMPv6 redirect messages are sent back to the sender by the Router in the redirect scenario is enabled on this interface.

If an IPv6 prefix is configured on the interface, the following information also displays.

Term	Definition
IPv6 Prefix is	The IPv6 prefix for the specified interface.
Preferred Lifetime	The amount of time the advertised prefix is a preferred prefix.
Valid Lifetime	The amount of time the advertised prefix is valid.
Onlink Flag	Shows whether the onlink flag is set (enabled) in the prefix.
Autonomous Flag	Shows whether the autonomous address-configuration flag (autoconfig) is set (enabled) in the prefix.

Command example:

```
(NETGEAR Switch) #show ipv6 interface brief
```

```

      Oper.
Interface  Mode      IPv6 Address/Length
-----
0/33      Enabled  FE80::211:88FF:FE2A:3E3C/128
              2033::211:88FF:FE2A:3E3C/64
0/17      Enabled  FE80::211:88FF:FE2A:3E3C/128
              2017::A42A:26DB:1049:43DD/128           [DHCP]
0/4 Enabled  FE80::211:88FF:FE2A:3E3C/128
              2001::211:88FF:FE2A:3E3C/64           [AUTO]
0/2      Disabled FE80::211:88FF:FE2A:3E3C/128           [TENT]

```

Command example:

```
(NETGEAR Switch) #show ipv6 interface 0/4
```

```

IPv6 is enabled
IPv6 Prefix is ..... fe80::210:18ff:fe00:1105/128
                      2001::1/64

Routing Mode..... Enabled
IPv6 Enable Mode..... Enabled
Administrative Mode..... Enabled
IPv6 Operational Mode..... Enabled
Bandwidth..... 10000 kbps
Interface Maximum Transmit Unit..... 1500
Router Duplicate Address Detection Transmits... 1
Address DHCP Mode..... Disabled
IPv6 Hop Limit Unspecified..... Enabled
Router Advertisement NS Interval..... 0
Router Advertisement Lifetime..... 1800
Router Advertisement Reachable Time..... 0
Router Advertisement Interval..... 600
Router Advertisement Managed Config Flag..... Disabled
Router Advertisement Other Config Flag..... Disabled
Router Advertisement Router Preference..... medium
Router Advertisement Suppress Flag..... Disabled
IPv6 Destination Unreachables..... Enabled
ICMPv6 Redirects..... Enabled

Prefix 2001::1/64
Preferred Lifetime..... 604800
Valid Lifetime..... 2592000
Onlink Flag..... Enabled
Autonomous Flag..... Enabled

```

show ipv6 interface (M4350 series switch)

M4350

Use this command to show the usability status of IPv6 interfaces and whether ICMPv6 Destination Unreachable messages may be sent.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

The **loopback** keyword with the *number* variable specifies the loopback interface directly and is a number in the range 0–7.

Format	show ipv6 interface [brief unit/slot/port vlan vlan-id loopback number]
Mode	Privileged EXEC

If you use the **brief** parameter, the following information displays for all configured IPv6 interfaces.

Term	Definition
Interface	The interface in the <i>unit/slot/port</i> format.
IPv6 Operational Mode	Shows whether the mode is enabled or disabled.
IPv6 Address/Length	Shows the IPv6 address and length on interfaces with IPv6 enabled.
Method	Indicates how each IP address was assigned. The field contains one of the following values: - DHCP. The address is leased from a DHCP server. - Manual. The address is manually configured. Global addresses with no annotation are assumed to be manually configured.

If you specify an interface, the following information also displays.

Term	Definition
Routing Mode	Shows whether IPv6 routing is enabled or disabled.
IPv6 Enable Mode	Shows whether IPv6 is enabled on the interface.
Administrative Mode	Shows whether the interface administrative mode is enabled or disabled.
Bandwidth	Shows bandwidth of the interface.
Interface Maximum Transmission Unit	The MTU size, in bytes.
Router Duplicate Address Detection Transmits	The number of consecutive duplicate address detection probes to transmit.
Address Autoconfigure Mode	Shows whether the autoconfigure mode is enabled or disabled.

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Address DHCP Mode	Shows whether the DHCPv6 client is enabled on the interface.
IPv6 Hop Limit Unspecified	Indicates if the router is configured on this interface to send Router Advertisements with unspecified (0) as the Current Hop Limit value.
Router Advertisement NS Interval	The interval, in milliseconds, between router advertisements for advertised neighbor solicitations.
Router Advertisement Lifetime	Shows the router lifetime value of the interface in router advertisements.
Router Advertisement Reachable Time	The amount of time, in milliseconds, to consider a neighbor reachable after neighbor discovery confirmation.
Router Advertisement Interval	The frequency, in seconds, that router advertisements are sent.
Router Advertisement Managed Config Flag	Shows whether the managed configuration flag is set (enabled) for router advertisements on this interface.
Router Advertisement Other Config Flag	Shows whether the other configuration flag is set (enabled) for router advertisements on this interface.
Router Advertisement Router Preference	Shows the router preference.
Router Advertisement Suppress Flag	Shows whether router advertisements are suppressed (enabled) or sent (disabled).
IPv6 Destination Unreachables	Shows whether ICMPv6 Destination Unreachable messages may be sent (enabled) or not (disabled). For more information, see ipv6 unreachable on page 1159 .
ICMPv6 Redirect	Specifies if ICMPv6 redirect messages are sent back to the sender by the Router in the redirect scenario is enabled on this interface.

If an IPv6 prefix is configured on the interface, the following information also displays.

Term	Definition
IPv6 Prefix is	The IPv6 prefix for the specified interface.
Preferred Lifetime	The amount of time the advertised prefix is a preferred prefix.
Valid Lifetime	The amount of time the advertised prefix is valid.
Onlink Flag	Shows whether the onlink flag is set (enabled) in the prefix.
Autonomous Flag	Shows whether the autonomous address-configuration flag (autoconfig) is set (enabled) in the prefix.

Command example:

```
(NETGEAR Switch) #show ipv6 interface brief
```

Interface	Oper. Mode	IPv6 Address/Length	
1/0/33	Enabled	FE80::211:88FF:FE2A:3E3C/128	
		2033::211:88FF:FE2A:3E3C/64	
2/0/17	Enabled	FE80::211:88FF:FE2A:3E3C/128	
		2017::A42A:26DB:1049:43DD/128	[DHCP]
0/4/1	Enabled	FE80::211:88FF:FE2A:3E3C/128	
		2001::211:88FF:FE2A:3E3C/64	[AUTO]
0/4/2	Disabled	FE80::211:88FF:FE2A:3E3C/128	[TENT]

Command example:

```
(NETGEAR Switch) #show ipv6 interface 0/4/1
```

```
IPv6 is enabled
IPv6 Prefix is ..... fe80::210:18ff:fe00:1105/128
                  2001::1/64

Routing Mode..... Enabled
IPv6 Enable Mode..... Enabled
Administrative Mode..... Enabled
IPv6 Operational Mode..... Enabled
Bandwidth..... 10000 kbps
Interface Maximum Transmit Unit..... 1500
Router Duplicate Address Detection Transmits... 1
Address DHCP Mode..... Disabled
IPv6 Hop Limit Unspecified..... Enabled
Router Advertisement NS Interval..... 0
Router Advertisement Lifetime..... 1800
Router Advertisement Reachable Time..... 0
Router Advertisement Interval..... 600
Router Advertisement Managed Config Flag..... Disabled
Router Advertisement Other Config Flag..... Disabled
Router Advertisement Router Preference..... medium
Router Advertisement Suppress Flag..... Disabled
IPv6 Destination Unreachables..... Enabled
ICMPv6 Redirects..... Enabled

Prefix 2001::1/64
Preferred Lifetime..... 604800
Valid Lifetime..... 2592000
Onlink Flag..... Enabled
Autonomous Flag..... Enabled
```

show ipv6 interface vlan

M4250

M4350

Use the show ipv6 interface vlan in Privileged EXEC mode to show the usability status of IPv6 VLAN interfaces.

Format	show ipv6 interface vlan <i>vlan-id</i> [<i>prefix</i>]
Mode	Privileged EXEC User EXEC
Parameter	Description
vlan-id	Valid VLAN ID
prefix	Display IPv6 Interface Prefix Information

show ipv6 nd raguard policy

M4250

M4350

This command shows the status of the IPv6 RA guard host mode on the switch. The output lists the ports and interfaces on which IPv6 RA guard host mode is enabled and the associated device roles.

Format	show ipv6 nd raguard policy
Modes	EXEC

Command example:

(NETGEAR Switch) # show ipv6 nd raguard policy

Configured Interfaces

Interface	Role
-----	-----
Gi1/0/1	Host

show ipv6 neighbors (M4250 series switch)

M4250

Use this command to display information about the IPv6 neighbors.

The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

Format	show ipv6 neighbor [<i>ipv6-address</i> interface { <i>slot/port</i> vlan <i>vlan-id</i> }]
Mode	Privileged EXEC
Term	Definition
Interface	The interface in <i>slot/port</i> format.
IPv6 Address	IPV6 address of neighbor or interface.
MAC Address	Link-layer Address.
IsRtr	Shows whether the neighbor is a router. If the value is TRUE, the neighbor is known to be a router, and FALSE otherwise. A value of FALSE might mean that routers are not always known to be routers.
Neighbor State	State of neighbor cache entry. Possible values are Incomplete, Reachable, Stale, Delay, Probe, and Unknown.
Last Updated	The time in seconds that has elapsed since an entry was added to the cache.
Type	The type of neighbor entry. The type is Static if the entry is manually configured and Dynamic if dynamically resolved.

show ipv6 neighbors (M4350 series switch)

M4350

Use this command to display information about the IPv6 neighbors.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

Format	show ipv6 neighbor [<i>ipv6-address</i> interface { <i>unit/slot/port</i> vlan <i>vlan-id</i> }]
Mode	Privileged EXEC
Term	Definition
Interface	The interface in <i>unit/slot/port</i> format.
IPv6 Address	IPV6 address of neighbor or interface.
MAC Address	Link-layer Address.

Term	Definition
IsRtr	Shows whether the neighbor is a router. If the value is TRUE, the neighbor is known to be a router, and FALSE otherwise. A value of FALSE might mean that routers are not always known to be routers.
Neighbor State	State of neighbor cache entry. Possible values are Incomplete, Reachable, Stale, Delay, Probe, and Unknown.
Last Updated	The time in seconds that has elapsed since an entry was added to the cache.
Type	The type of neighbor entry. The type is Static if the entry is manually configured and Dynamic if dynamically resolved.

clear ipv6 neighbors

M4250

M4350

Use this command to clear all entries IPv6 neighbor table or an entry on a specific interface. Use the optional *unit/slot/port* parameter to specify an interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>clear ipv6 neighbors [unit/slot/port]</code>
Mode	Privileged EXEC

show ipv6 route (M4250 series switch)

M4250

This command displays the IPv6 routing table. The *ipv6-address* specifies a specific IPv6 address for which the best-matching route is displayed. The *ipv6-prefix/ipv6-prefix-length* specifies a specific IPv6 network for which the matching route is displayed.

The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

The **ospf**, **connected** or **static keyword** specifies the protocol that installed the routes.

The **all** keyword specifies that all routes including best and non-best routes are displayed. Otherwise, only the best routes are displayed.

Note: If you use the **connected** keyword, the **all** option is not available because there are no best or “nonbest” connected routes.

Format	<code>show ipv6 route [ipv6-address [static connected] {{ipv6-prefix/ipv6-prefix-length slot/port vlan vlan-id} [static connected] [static connected] summary} [all] all]</code>

Modes	Privileged EXEC User EXEC

Term	Definition

Route Codes	The key for the routing protocol codes that might appear in the routing table output.

The **show ipv6 route** command displays the routing tables in the following format:

Codes: C - connected, S - static

The columns for the routing table display the following information.

Term	Definition

Code	The code for the routing protocol that created this routing entry.

Default Gateway	The IPv6 address of the default gateway. When the system does not have a more specific route to a packet's destination, it sends the packet to the default gateway.

IPv6-Prefix/IPv6-Prefix-Length	The IPv6-Prefix and prefix-length of the destination IPv6 network corresponding to this route.

Preference/Metric	The administrative distance (preference) and cost (metric) associated with this route. An example of this output is [1/0], where 1 is the preference and 0 is the metric.

Tag	The decimal value of the tag associated with a redistributed route, if it is not 0.

Next-Hop	The outgoing router IPv6 address to use when forwarding traffic to the next router (if any) in the path toward the destination.

Route-Timestamp	The last updated time for dynamic routes. The format of Route-Timestamp is: Days:Hours:Minutes if days >= 1 Hours:Minutes:Seconds if days < 1

Interface	The outgoing router interface to use when forwarding traffic to the next destination. For reject routes, the next hop interface is the Null0 interface.

T	A flag appended to an IPv6 route to indicate that it is an ECMP route, but only one of its next hops has been installed in the forwarding table. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop. Such truncated routes are identified by a T after the interface name.

To administratively control the traffic destined to a particular network and prevent it from being forwarded through the switch, you can configure a static reject route on the switch.

Such traffic would be discarded and an ICMP destination unreachable message is sent back to the source. This configuration is typically used for preventing routing loops.

Command example:

```
(NETGEAR Switch) #show ipv6 route

IPv6 Routing Table - 3 entries
Codes: C - connected, S - static

S   2001::/64 [10/0] directly connected,   Null0
C   2003::/64 [0/0]
    via ::,   0/11
S   2005::/64 [1/0]
    via 2003::2,   0/11
C 5001::/64 [0/0]
    via ::,   0/5
```

Command example:

The following example displays a truncated route:

```
(NETGEAR Switch) #show ipv6 route

IPv6 Routing Table - 2 entries
Codes: C - connected, S - static, 6To4 - 6to4 Route

C   2001:db9:1::/64 [0/0]
    via ::,   0/1
```

show ipv6 route (M4350 series switch)

M4350

This command displays the IPv6 routing table. The *ipv6-address* specifies a specific IPv6 address for which the best-matching route is displayed. The *ipv6-prefix/ipv6-prefix-length* specifies a specific IPv6 network for which the matching route is displayed.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

The **ospf**, **connected** or **static keyword** specifies the protocol that installed the routes.

The **all** keyword specifies that all routes including best and non-best routes are displayed. Otherwise, only the best routes are displayed.

Note: If you use the **connected** keyword, the **all** option is not available because there are no best or “nonbest” connected routes.

Format	<code>show ipv6 route [ipv6-address [ospf static connected] {{ipv6-prefix/ipv6-prefix-length unit/slot/port vlan vlan-id} [ospf static connected] [ospf static connected] summary} [all] all]</code>
Modes	Privileged EXEC User EXEC

Term	Definition
Route Codes	The key for the routing protocol codes that might appear in the routing table output.

The **show ipv6 route** command displays the routing tables in the following format:

Codes: C - connected, S - static

The columns for the routing table display the following information.

Term	Definition
Code	The code for the routing protocol that created this routing entry.
Default Gateway	The IPv6 address of the default gateway. When the system does not have a more specific route to a packet's destination, it sends the packet to the default gateway.
IPv6-Prefix/IPv6-Prefix-Length	The IPv6-Prefix and prefix-length of the destination IPv6 network corresponding to this route.
Preference/Metric	The administrative distance (preference) and cost (metric) associated with this route. An example of this output is [1/0], where 1 is the preference and 0 is the metric.
Tag	The decimal value of the tag associated with a redistributed route, if it is not 0.
Next-Hop	The outgoing router IPv6 address to use when forwarding traffic to the next router (if any) in the path toward the destination.
Route-Timestamp	The last updated time for dynamic routes. The format of Route-Timestamp is: Days:Hours:Minutes if days >= 1 Hours:Minutes:Seconds if days < 1
Interface	The outgoing router interface to use when forwarding traffic to the next destination. For reject routes, the next hop interface is the Null0 interface.
T	A flag appended to an IPv6 route to indicate that it is an ECMP route, but only one of its next hops has been installed in the forwarding table. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop. Such truncated routes are identified by a T after the interface name.

To administratively control the traffic destined to a particular network and prevent it from being forwarded through the switch, you can configure a static reject route on the switch.

Such traffic would be discarded and an ICMP destination unreachable message is sent back to the source. This configuration is typically used for preventing routing loops.

Command example:

```
(NETGEAR Switch) #show ipv6 route

IPv6 Routing Table - 3 entries
Codes: C - connected, S - static

S   2001::/64 [10/0] directly connected,   Null0
C   2003::/64 [0/0]
    via ::,   0/11
S   2005::/64 [1/0]
    via 2003::2,   0/11
C 5001::/64 [0/0]
    via ::,   0/5
```

Command example:

The following example displays a truncated route:

```
(NETGEAR Switch) #show ipv6 route

IPv6 Routing Table - 2 entries
Codes: C - connected, S - static, 6To4 - 6to4 Route

C   2001:db9:1::/64 [0/0]
    via ::,   0/1
```

show ipv6 route ecmp-groups

M4250

M4350

This command reports all current ECMP groups in the IPv6 routing table. An ECMP group is a set of two or more next hops used in one or more routes. The groups are numbered arbitrarily from 1 to n. The output indicates the number of next hops in the group and the number of routes that use the set of next hops. The output lists the IPv6 address and outgoing interface of each next hop in each group.

Format	show ipv6 route ecmp-groups
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show ipv6 route ecmp-groups
ECMP Group 1 with 2 next hops (used by 1 route)
    2001:DB8:1::1 on interface 2/1
    2001:DB8:2::14 on interface 2/2
ECMP Group 2 with 3 next hops (used by 1 route)
    2001:DB8:4::15 on interface 2/32
    2001:DB8:7::12 on interface 2/33
    2001:DB8:9::45 on interface 2/34
```

show ipv6 route hw-failure**M4250****M4350**

This command displays the routes that were not added to the hardware because of hash errors or because the table was full.

Format	show ipv6 route hw-failure

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show ipv6 route hw-failure
IPv6 Routing Table - 4 entries
Codes: C - connected, S - static, 6To4 - 6to4 Route, K - kernel
P - Net Prototype
P    3001::/64 [0/1]
      via 2001::4,    00h:00m:04s,    0/1  hw-failure
P    3001:0:0:1::/64 [0/1]
      via 2001::4,    00h:00m:04s,    0/1  hw-failure
P    3001:0:0:2::/64 [0/1]
      via 2001::4,    00h:00m:04s,    0/1  hw-failure
P    3001:0:0:3::/64 [0/1]
      via 2001::4,    00h:00m:04s,    0/1  hw-failure
```

show ipv6 route kernel

M4250

M4350

This command displays kernel routes, if any exist. The optional **a11** keyword displays the best and “nonbest” kernel routes.

Format	show ipv6 route kernel [all]

Mode	Privileged EXEC

show ipv6 route 6to4

M4250

M4350

This command displays IPv6-over-IPv4 tunnels that are manually configured in the switch.

Format	show ipv6 route 6to4

Mode	Privileged EXEC

show ipv6 route net-prototype

M4250

M4350

This command displays the net prototype routes. The output displays the net prototype routes with a P.

Format	show ipv6 route net-prototype

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show ipv6 route net-prototype
IPv6 Routing Table - 2 entries
Codes: C - connected, S - static, 6To4 - 6to4 Route, K - kernel
       P - Net Prototype
P    3001::/64 [0/1]
      via 2001::4,    00h:00m:04s,    0/1
P    3001:0:0:1::/64 [0/1]
      via 2001::4,    00h:00m:04s,    0/1
```

show ipv6 route preferences

M4250

M4350

Use this command to show the preference value associated with the type of route. Lower numbers have a greater preference. A route with a preference of 255 cannot be used to forward traffic.

Format	show ipv6 route preferences

Mode	Privileged EXEC

Term	Definition
Local	Preference of directly-connected routes.
Static	Preference of static routes.

show ipv6 route summary

M4250

M4350

This command displays a summary of the state of the routing table. With the optional **a11** keyword, some statistics, such as the number of routes from each source, include counts for alternate routes. An alternate route is a route that is not the most preferred route to its destination and therefore is not installed in the forwarding table. To include only the number of best routes, do not use the optional **a11** keyword.

Format	show ipv6 route summary [all]

Modes	Privileged EXEC User EXEC

Term	Definition
Connected Routes	Total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
Reject Routes	Total number of reject routes installed by all protocols.
Net Prototype Routes	The total number of net prototype routes.
Number of Prefixes	Summarizes the number of routes with prefixes of different lengths.
Total Routes	The total number of routes in the routing table.
Best Routes	The number of best routes currently in the routing table. This number only counts the best route to each destination.

Term	Definition
Alternate Routes	The number of alternate routes currently in the routing table. An alternate route is a route that was not selected as the best route to its destination.
Route Adds	The number of routes that have been added to the routing table.
Route Modifies	The number of routes that have been changed after they were initially added to the routing table.
Route Deletes	The number of routes that have been deleted from the routing table.
Unresolved Route Adds	The number of route adds that failed because none of the route's next hops were on a local subnet. Note that static routes can fail to be added to the routing table at startup because the routing interfaces are not yet up. This counter gets incremented in this case. The static routes are added to the routing table when the routing interfaces come up.
Invalid Route Adds	The number of routes that failed to be added to the routing table because the route was invalid. A log message is written for each of these failures.
Failed Route Adds	The number of routes that failed to be added to the routing table because of a resource limitation in the routing table.
Hardware Failed Route Adds	The number of routes that failed to be inserted into the hardware because of a hash error or a table-full condition.
Reserved Locals	The number of routing table entries reserved for a local subnet on a routing interface that is down. Space for local routes is always reserved so that local routes can be installed when a routing interface bounces.
Unique Next Hops	The number of distinct next hops used among all routes currently in the routing table. These include local interfaces for local routes and neighbors for indirect routes.
Unique Next Hops High Water	The highest count of unique next hops since counters were last cleared.
Next Hop Groups	The current number of next hop groups in use by one or more routes. Each next hop group includes one or more next hops.
Next Hop Groups High Water	The highest count of next hop groups since counters were last cleared.
ECMP Groups	The number of next hop groups with multiple next hops.
ECMP Routes	The number of routes with multiple next hops currently in the routing table.
Truncated ECMP Routes	The number of ECMP routes that are currently installed in the forwarding table with just one next hop. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop.
ECMP Retries	The number of ECMP routes that have been installed in the forwarding table after initially being installed with a single next hop.
Routes with n Next Hops	The current number of routes with each number of next hops.

Command example:

```
(NETGEAR Switch) #show ipv6 route summary

Connected Routes..... 4
Static Routes..... 0
6To4 Routes..... 0
Reject Routes..... 0
Total routes..... 17

Best Routes (High)..... 17 (17)
Alternate Routes..... 0
Route Adds..... 44
Route Deletes..... 27
Unresolved Route Adds..... 0
Invalid Route Adds..... 0
Failed Route Adds..... 0
Reserved Locals..... 0

Unique Next Hops (High)..... 8 (8)
Next Hop Groups (High)..... 8 (8)
ECMP Groups (High)..... 3 (3)
ECMP Routes..... 12
Truncated ECMP Routes..... 0
ECMP Retries..... 0
Routes with 1 Next Hop..... 5
Routes with 2 Next Hops..... 1
Routes with 3 Next Hops..... 1
Routes with 4 Next Hops..... 10

Number of Prefixes:
/64: 17
```

clear ipv6 route counters**M4250****M4350**

The command resets to zero the IPv6 routing table counters reported in the command `show ipv6 route summary` on page 1177. The command only resets event counters. Counters that report the current state of the routing table, such as the number of routes of each type, are not reset.

Format	clear ipv6 route counters
Mode	Privileged Exec

clear ipv6 snooping counters

M4250**M4350**

This command clears the counters that are associated with the IPv6 RA guard host mode.

Format	clear ipv6 snooping counters

Modes	EXEC Global Config

Command example:

```
(NETGEAR Switch) # clear ipv6 snooping counters
```

show ipv6 snooping counters

M4250**M4350**

This command displays the counters that are associated with the IPv6 RA guard host mode. The output displays the number of router advertisements and router redirect packets that are dropped globally because of the IPv6 RA guard host mode.

Format	show ipv6 snooping counters

Modes	EXEC Global Config

Command example:

```
(NETGEAR Switch) # show ipv6 snooping counters
```

```
IPv6 Dropped Messages
RA (Router Advertisement - ICMP type 134):  431
REDIR (Router Redirect - ICMP type 137):    6599
RA                                     Redir
-----                             -
0                                     0
```

show ipv6 vlan

M4250

M4350

This command displays IPv6 VLAN routing interface addresses.

Format	show ipv6 vlan
Modes	Privileged EXEC User EXEC
Term	Definition
MAC Address used by Routing VLANs	Shows the MAC address.

The rest of the output for this command is displayed in a table with the following column headings.

Column Headings	Definition
VLAN ID	The VLAN ID of a configured VLAN.
Logical Interface	The interface that is associated with the VLAN ID.
IPv6 Address/Prefix Length	The IPv6 prefix and prefix length associated with the VLAN ID.

show ipv6 traffic

M4250

M4350

Use this command to show traffic and statistics for IPv6 and ICMPv6. Specify a logical or loopback interface to view information about traffic on a specific interface.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

If you do not specify an interface, the command displays information about traffic on all interfaces.

Format	show ipv6 traffic [<i>unit/slot/port</i> <i>vlan vlan-id</i> <i>loopback loopback-id</i>]
Mode	Privileged EXEC

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Total Datagrams Received	Total number of input datagrams received by the interface, including those received in error.
Received Datagrams Locally Delivered	Total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter increments at the interface to which these datagrams were addressed, which might not necessarily be the input interface for some of the datagrams.
Received Datagrams Discarded Due To Header Errors	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, etc.
Received Datagrams Discarded Due To MTU	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	Number of input datagrams discarded because no route could be found to transmit them to their destination.
Received Datagrams With Unknown Protocol	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter increments at the interface to which these datagrams were addressed, which might not be necessarily the input interface for some of the datagrams.
Received Datagrams Discarded Due To Invalid Address	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 (for example, addresses with unallocated prefixes). For entities which 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	Number of input datagrams discarded because datagram frame didn't carry enough data.
Received Datagrams Discarded Other	Number of input IPv6 datagrams for which no problems were encountered to prevent their continue processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include datagrams discarded while awaiting re-assembly.
Received Datagrams Reassembly Required	Number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter increments at the interface to which these fragments were addressed, which might not be necessarily the input interface for some of the fragments.
Datagrams Successfully Reassembled	Number of IPv6 datagrams successfully reassembled. Note that this counter increments 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	Number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in by combining them as they are received. This counter increments at the interface to which these fragments were addressed, which might not be necessarily the input interface for some of the fragments.

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Datagrams Forwarded	Number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface increments.
Datagrams Locally Transmitted	Total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in <code>ipv6IfStatsOutForwDatagrams</code> .
Datagrams Transmit Failed	Number of output IPv6 datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in <code>ipv6IfStatsOutForwDatagrams</code> if any such packets met this (discretionary) discard criterion.
Fragments Created	Number of output datagram fragments that have been generated as a result of fragmentation at this output interface.
Datagrams Successfully Fragmented	Number of IPv6 datagrams that have been successfully fragmented at this output interface.
Datagrams Failed To Fragment	Number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.
Fragments Created	The number of fragments that were created.
Multicast Datagrams Received	Number of multicast packets received by the interface.
Multicast Datagrams Transmitted	Number of multicast packets transmitted by the interface.
Total ICMPv6 messages received	Total number of ICMP messages received by the interface which includes all those counted by <code>ipv6IfIcmpInErrors</code> . Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.
ICMPv6 Messages with errors	Number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
ICMPv6 Destination Unreachable Messages Received	Number of ICMP Destination Unreachable messages received by the interface.
ICMPv6 Messages Prohibited Administratively Received	Number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.
ICMPv6 Time Exceeded Messages Received	Number of ICMP Time Exceeded messages received by the interface.
ICMPv6 Parameter Problem Messages Received	Number of ICMP Parameter Problem messages received by the interface.
ICMPv6 Packet Too Big Messages Received	Number of ICMP Packet Too Big messages received by the interface.
ICMPv6 Echo Request Messages Received	Number of ICMP Echo (request) messages received by the interface.

Term	Definition
ICMPv6 Echo Reply Messages Received	Number of ICMP Echo Reply messages received by the interface.
ICMPv6 Router Solicit Messages Received	Number of ICMP Router Solicit messages received by the interface.
ICMPv6 Router Advertisement Messages Received	Number of ICMP Router Advertisement messages received by the interface.
ICMPv6 Neighbor Solicit Messages Received	Number of ICMP Neighbor Solicit messages received by the interface.
ICMPv6 Neighbor Advertisement Messages Received	Number of ICMP Neighbor Advertisement messages received by the interface.
ICMPv6 Redirect Messages Received	Number of Redirect messages received by the interface.
ICMPv6 Group Membership Query Messages Received	Number of ICMPv6 Group Membership Query messages received by the interface.
ICMPv6 Group Membership Response Messages Received	Number of ICMPv6 Group Membership response messages received by the interface.
ICMPv6 Group Membership Reduction Messages Received	Number of ICMPv6 Group Membership reduction messages received by the interface.
Total ICMPv6 Messages Transmitted	Total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.
ICMPv6 Messages Not Transmitted Due To Error	Number of ICMP messages which this interface did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IPv6 to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
ICMPv6 Destination Unreachable Messages Transmitted	Number of ICMP Destination Unreachable messages sent by the interface.
ICMPv6 Messages Prohibited Administratively Transmitted	Number of ICMP destination unreachable/communication administratively prohibited messages sent.
ICMPv6 Time Exceeded Messages Transmitted	Number of ICMP Time Exceeded messages sent by the interface.
ICMPv6 Parameter Problem Messages Transmitted	Number of ICMP Parameter Problem messages sent by the interface.
ICMPv6 Packet Too Big Messages Transmitted	Number of ICMP Packet Too Big messages sent by the interface.
ICMPv6 Echo Request Messages Transmitted	Number of ICMP Echo (request) messages sent by the interface. ICMP echo messages sent.
ICMPv6 Echo Reply Messages Transmitted	Number of ICMP Echo Reply messages sent by the interface.

Term	Definition
ICMPv6 Router Solicit Messages Transmitted	Number of ICMP Router Solicitation messages sent by the interface.
ICMPv6 Router Advertisement Messages Transmitted	Number of ICMP Router Advertisement messages sent by the interface.
ICMPv6 Neighbor Solicit Messages Transmitted	Number of ICMP Neighbor Solicitation messages sent by the interface.
ICMPv6 Neighbor Advertisement Messages Transmitted	Number of ICMP Neighbor Advertisement messages sent by the interface.
ICMPv6 Redirect Messages Received	Number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
ICMPv6 Group Membership Query Messages Transmitted	Number of ICMPv6 Group Membership Query messages sent.
ICMPv6 Group Membership Response Messages Transmitted	Number of ICMPv6 Group Membership Response messages sent.
ICMPv6 Group Membership Reduction Messages Transmitted	Number of ICMPv6 Group Membership Reduction messages sent.
ICMPv6 Duplicate Address Detects	Number of duplicate addresses detected by the interface.

show ipv6 protocols

M4350

This command lists a summary of the configuration and status for the active IPv6 routing protocols. The command lists routing protocols that are configured and enabled. If you select the optional **ospf** keyword, the command output is limited to that protocol.

Format	<code>show ipv6 protocols [ospf]</code>
Mode	Privileged Exec

Parameter	Description
Routing Protocol	OSPFv3.
Router ID	The router ID configured for OSPFv3.
OSPF Admin Mode	Whether OSPF is enabled or disabled globally.
Maximum Paths	The maximum number of next hops in an OSPF route.
Default Route Advertise	Whether OSPF is configured to originate a default route.
Always	Whether default advertisement depends on having a default route in the common routing table.

Parameter	Description
Metric	The metric configured to be advertised with the default route.
Metric Type	The metric type for the default route.

Command example:

```
(NETGEAR Switch) #show ipv6 protocols
```

```

Routing Protocol ..... OSPFv3
Router ID ..... 1.1.1.1
OSPF Admin Mode ..... Enable
Maximum Paths ..... 4
Distance ..... Intra 110 Inter 110 Ext 110

Default Route Advertise ..... Disabled
Always ..... FALSE
Metric ..... Not configured
Metric Type ..... External Type 2

Number of Active Areas ..... 0 (0 normal, 0 stub, 0 nssa)
ABR Status ..... Disable
ASBR Status ..... Disable

```

show ipv6 prefix-list**M4250****M4350**

This command displays configuration and status for a specific IPv6 prefix list.

Format `show ipv6 prefix-list {listname [ipv6-prefix/prefix-length [longer | first-match]] | listname seq 1-4294967294 | detail [listname] | summary [listname]}`

Mode Privileged Exec

Parameter	Description
<i>listname</i>	The name of the prefix list.
<i>ipv6-prefix/prefix-length</i>	The IPv6 network number and length (in bits) of the network mask.
<i>first-match</i>	Displays the entry of a prefix list that matches the specified network and length.
<i>longer</i>	Displays all entries of a prefix list that are more specific than the specified network and length.
seq <i>sequence-number</i>	The sequence number for the prefix list.

Parameter	Description
detail	Displays detailed information about all prefix lists.
summary	Displays summarized information about all prefix lists.

The command output includes the following information.

Field	Description
Count	The number of entries in the prefix list.
Range Entries	The number of entries that match the input range.
Ref Count	The number of entries that reference the prefix list.
Seq	The sequence number of the entry in the prefix list.
Permit/Deny	The permit or deny action that is taken.
Sequences	The range of sequence numbers for the entries in the prefix list,
Hit Count	The number of matches for the prefix list.

Command example:

```
(NETGEAR Switch)#show ipv6 prefix-list applelist
ipv6 prefix-list applelist:
count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
seq 5 deny 5F00::/8 le 128
seq 10 deny ::/0
seq 15 deny ::/1
seq 20 deny ::/2
seq 25 deny ::/3 ge 4
seq 30 permit ::/0 le 128
```

Command example:

```
(NETGEAR Switch)#show ipv6 prefix-list summary applelist
ipv6 prefix-list applelist:
count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
```

Command example:

```
(NETGEAR Switch)#show ipv6 prefix-list detail applelist
ipv6 prefix-list applelist:
count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
seq 5 deny 5F00::/8 le 128 (hit count: 0, refcount: 1)
seq 10 deny ::/0 (hit count: 0, refcount: 1)
seq 15 deny ::/1 (hit count: 0, refcount: 1)
seq 20 deny ::/2 (hit count: 0, refcount: 1)
seq 25 deny ::/3 ge 4 (hit count: 0, refcount: 1)
seq 30 permit ::/0 le 128 (hit count: 240664, refcount: 0)
```

clear ipv6 statistics

M4250

M4350

Use this command to clear IPv6 statistics for all interfaces or for a specific interface, including loopback interfaces. IPv6 statistics display in the output of the **show ipv6 traffic** command. If you do not specify an interface, the counters for all IPv6 traffic statistics reset to zero.

Format	<code>clear ipv6 statistics [unit/slot/port loopback loopback-id vlan vlan-id]</code>
Mode	Privileged EXEC

IPv6 Policy-Based Routing Commands

The following commands that are described for IPv4 traffic in [Routing Policy Commands on page 946](#) can also be used for IPv6 traffic:

- **match-length**
- **match-mac-list**
- **set interface**

ipv6 policy

This command specifies a route map that must be used for policy-based IPv6 routing on an interface.

M4250

M4350

The *route-map-name* argument specifies the name of the route map that must be used for policy routing. It must match a map tag specified by a **route-map** command. If you try to apply a route-map name that is not yet created, an error message is displayed.

Format	<code>ipv6 policy route-map route-map-name</code>
Mode	Interface Config

Usage Guidelines

A route-map statement must contain eligible match and set conditions for policy-based routing to be applied to hardware:

- Valid match conditions: **match ipv6 address acl**, **match mac-list**, **match length**
- Valid set conditions: **set ipv6 next-hop**, **set ipv6 default next-hop**, **set ipv6 precedence**

A route map must contain at least one match condition and one set condition. If it does not, the route map is not applied to hardware.

A route map and a Diffserv policy cannot function together on the same interface. When you apply a route map on a VLAN interface and a DiffServ policy on a member port of the same VLAN interface, the port policy has priority over the VLAN policy.

The same route map cannot be applied using both the **ip policy** and **ipv6 policy** commands on an interface. When a route map has both IPv4 and IPv6 statements provisioned and you apply the route map using the **ipv6 policy** command, the IPv4 statements in the route map do not take effect, and a message is displayed.

Command example:

```
(NETGEAR Switch) (Interface vlan 40)#ipv6 policy route-map rm4
```

no ipv6 policy

This command disables a specified route map on an interface.

Format	no ipv6 policy route-map <i>route-map-name</i>

Mode	Global Config

ipv6 prefix-list description

M4250

M4350

This command adds an IPv6 prefix list with a description, or adds a description to an existing IPv6 prefix list, but does not configure the IPv6 address in the prefix list. To configure the IPv6 address in the prefix list, use the **ipv6 prefix-list** command.

Format	ipv6 prefix-list <i>list-name</i> description <i>text</i>

Mode	Global Config

Parameter	Description
<i>prefix-list-name</i>	The text name of the prefix list. The name can be up to 32 characters.
description <i>text</i>	A description of the prefix list. The description can be up to 80 characters in length.

no ipv6 prefix-list description

This command removes the description from an IPv6 prefix list.

Format	no ipv6 prefix-list <i>list-name</i> description

Mode	Global Config

ipv6 prefix-list

M4250

M4350

To create a prefix list or add a prefix list entry, use the **ipv6 prefix-list** command in Global Configuration mode. Prefix lists allow matching of route prefixes with those specified in the prefix list. Each prefix list includes a sequence of prefix list entries ordered by their sequence numbers. A router or switch sequentially examines each prefix list entry to determine if the route's prefix matches that of the entry. An empty or nonexistent prefix list permits all prefixes. An implicit deny is assumed if a prefix does not match any entries of a prefix list. Once a match or deny occurs, the router or switch does not go through the rest of the list.

Up to 128 prefix lists may be configured. The maximum number of statements allowed in prefix list is 64.

To add a description to the IPv6 prefix list, use the **ipv6 prefix-list description** command.

To renumber an IPv6 prefix list, use the **ipv6 prefix-list renumber** command.

Default	No prefix lists are configured by default. When neither the ge nor the le option is configured, the destination prefix must match the network/length exactly. If the ge option is configured without the le option, any prefix with a network mask greater than or equal to the ge value is considered a match. Similarly, if the le option is configured without the ge option, a prefix with a network mask less than or equal to the le value is considered a match.
Format	<code>ipv6 prefix-list list-name [seq number] {permit deny}</code> <code>ipv6-prefix/prefix-length [ge length] [le length]</code>
Mode	Global Configuration
Parameter	Description
<i>list-name</i>	The text name of the prefix list. The name can be up to 32 characters.
<i>seq number</i>	(Optional) The sequence number for this prefix list statement. Prefix list statements are ordered from lowest sequence number to highest and applied in that order. If you do not specify a sequence number, the system will automatically select a sequence number five larger than the last sequence number in the list. Two statements may not be configured with the same sequence number. The value range for <i>number</i> is from 1 to 4,294,967,294.
permit	Permit routes whose destination prefix matches the statement.
deny	Deny routes whose destination prefix matches the statement.
<i>ipv6-prefix/prefix-length</i>	Specifies the match criteria for routes being compared to the prefix list statement. The <i>ipv6-prefix</i> can be any valid IP prefix. The length is any IPv6 prefix length from 0 to 32.

Parameter	Description
<i>ge length</i>	(Optional) If this option is configured, then a prefix is only considered a match if its network mask length is greater than or equal to this value. This value must be longer than the network length and less than or equal to 32.
<i>le length</i>	(Optional) If this option is configured, then a prefix is only considered a match if its network mask length is less than or equal to this value. This value must be longer than the ge length and less than or equal to 32.

no ip prefix-list

To delete a prefix list or a statement in a prefix list, use the **no ip prefix-list** command. The **no ip prefix-list list-name** command deletes the entire prefix list. To remove an individual statement from a prefix list, you must specify the statement exactly, with all its options.

Format	<code>no ipv6 prefix-list list-name [seq number] {permit deny}</code> <code>ipv6-prefix/prefix-length [ge length] [le length]</code>
Mode	Global Configuration

ipv6 prefix-list renumber

M4250

M4350

You can renumber the sequence numbers of the statements in an IPv6 prefix list. You need to specify the renumber interval and the number of the first statement. where the renumbering must start.

Format	<code>ipv6 prefix-list list-name renumber renumber-interval first-statement-number</code>
Mode	Global Configuration

Parameter	Description
<i>list-name</i>	The text name of the prefix list. The name can be up to 32 characters.
<i>renumber-interval</i>	The renumber interval. The range is from 1 to 100.
<i>first-statement-number</i>	The first statement where renumbering must start. The range is from 1 to 1000.

clear ipv6 prefix-list

M4250

M4350

This command resets and clears the IPv6 prefix-list counter. The counter indicates the number of matches to a specific prefix list entry.

Format	<code>clear ipv6 prefix-list [prefix-list-name] [ipv6-prefix/prefix-length]</code>
Mode	Privileged Config
Parameter	Description
<i>prefix-list-name</i>	(Optional) The name of the prefix list for which the counter must be cleared.
<i>ipv6-prefix/prefix-length</i>	(Optional) The IPv6 prefix number and length (in bits) of the network mask for which the counter must be cleared.

match ipv6 address

M4250

M4350

Use this command to configure a route map that must match based on the match criteria configured in one or more existing IPv6 access lists (ACLs). (If you specify an IPv6 ACL name or number that does not exist, an error message is displayed.)

Actions that are configured in an IPv6 ACL are applied with other actions involved in the route map. When an IPv6 ACL referenced by a route-map is removed or rules are added or deleted from that ACL, the configuration is rejected. However, you can add ACLs to or removing ACLs from a route map that is attached to an interface.

If you specify a a list of IPv6 ACLs and a packet matches at least one of these ACL match criteria, the corresponding set actions in the route map are applied to packet.

If you specify duplicate IPv6 ACL numbers or names in this command, the duplicate configuration is ignored.

To enter the Route Map Configuration mode, from the Config mode, enter the **route-map map-tag** command.

Default	No match criteria are defined by default.
Format	<code>match ipv6 address {access-list-number access-list-name} [...access-list-number access-list-name]</code>
Mode	Route Map Configuration

Parameter	Description
<i>access-list-number</i>	The IPv6 ACL number that identifies an ACL configured through access-list CLI configuration commands. This number is from 1 to 99 for a standard ACL. This number is from 100 to 199 for an extended ACL. You can specify a maximum of four ACLs in this match clause.
<i>access-list-name</i>	The IPv6 ACL name that identifies the named IPv6 ACL. The name can be up to 31 characters in length. You can specify a maximum of four ACLs in this match clause.

Command example:

Following command sequence shows how to first create an ACL and then a route map with a match clause on the ACL number and apply that route map to an interface.

```
(NETGEAR Switch) (Config)#ipv6 access-list acl2
(NETGEAR Switch) (Config-ipv6-acl)#permit ipv6 1001::1 any
(NETGEAR Switch) (Config-ipv6-acl)#exit
(NETGEAR Switch) (Config)#route-map rm1 permit 40
(NETGEAR Switch) (route-map)#match ipv6 address acl2
(NETGEAR Switch) (config-route-map)#set ipv6 default next-hop 2001::2
(NETGEAR Switch) (config)#interface 0/1
(NETGEAR Switch) (Interface 1/0/4)#ip address 10.1.1.1 255.255.255.0
(NETGEAR Switch) (Interface 1/0/4)#ipv6 policy route-map rm1
```

The results are the following:

- The **ipv6 policy route-map rm1** command is applied to interface 1/0/4. All packets that enter on that interface are policy-routed if a match is made per the IPv6 ACL.
- Sequence number 40 in route map rm1 is used to match all packets sourced from host 1001::1. If there is a match, and if the switch has no explicit route for the packet destination, the packets are sent to next-hop address 2001::2.
- The rest of the packets are forwarded per normal L3 destination-based routing.

no match ipv6 address

Use the **no match ipv6 address** command to delete a match statement from a route map.

Format	<code>no match ipv6 address [...access-list-number access-list-name]</code>
Mode	Route Map Configuration

set ipv6 next-hop

M4250

M4350

Use this command to specify the adjacent next-hop router in the path toward the destination to which the packets must be forwarded. If more than one IPv6 address is specified, the first IPv6 address associated with an interface that is up is used to route the packets.

To specify a next-hop IPv6 address that is a link-local address, use the **interface** *unit/slot/port* or **interface vlan** *vlan-id* options.

You can specify up four IPv6 addresses for next-hop routers. However, if you use the **interface** or **interface vlan** keyword, you can optionally specify one IPv6 address for a next-hop router.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	<code>set ipv6 next-hop {interface <i>unit/slot/port</i> [<i>next-hop-ipv6-address</i>] vlan <i>vlan-id</i> [<i>next-hop-ipv6-address</i>] <i>next-hop-ipv6-address</i> [...<i>next-hop-ipv6-address</i>] }</code>

Mode	Route Map Configuration

Parameter	Description
<i>unit/slot/port</i>	If the IPv6 address is a link-local address, specify a routing interface (or VLAN ID).
<i>vlan-id</i>	If the IPv6 address is a link-local address, specify a VLAN ID in the range from 1 to 4093 (or an interface).
<i>next-hop-ipv6-address</i>	The global IPv6 address of the next-hop router to which packets are routed. This address must be the address of an adjacent router. You can specify up to four IPv6 addresses. However, if you use the interface or interface vlan keyword, you can optionally specify one IPv6 address for a next-hop router.

Usage guidelines

This command affects all incoming packet types and is always used if enabled and configured. The switch checks the NDP table to see if the next-hop router is resolved, and if so, packets are forwarded to the next-hop router.

In a route-map statement, the **set ipv6 next-hop** and **set ipv6 default next-hop** commands are mutually exclusive. However, you can configure the **set ipv6 default next-hop** command in a separate route-map statement.

Command example:

```
(NETGEAR Switch) (Config) #route-map RouteMapName
(NETGEAR Switch) (route-map) #set ipv6 next-hop 3333::2
```


no set ipv6 next-hop

Use this command to delete a next-hop match statement from a route map.

Format	no set ipv6 next-hop {interface <i>unit/slot/port</i> [<i>next-hop-ipv6-address</i>] vlan <i>vlan-id</i> [<i>next-hop-ipv6-address</i>] <i>next-hop-ipv6-address</i> [... <i>next-hop-ipv6-address</i>]}
Mode	Route Map Configuration

set ipv6 default next-hop

M4250

M4350

Use this command to specify a list of default next-hop IPv6 addresses. If more than one IPv6 address is specified, the first specified next-hop IPv6 address that is adjacent to the router is used. The other specified IPv6 addresses are tried in turn.

To specify a next-hop IPv6 address that is a link-local address, use the **interface** *unit/slot/port* or **interface** **vlan** *vlan-id* options.

You can specify up to four IPv6 addresses for next-hop routers. However, if you use the **interface** or **interface** **vlan** option, you can optionally specify a single IPv6 address for a next-hop router.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Default	No match criteria are defined by default.
Format	set ipv6 default next-hop {interface { <i>unit/slot/port</i> <i>vlan</i> <i>vlan-id</i> } [... <i>default-next-hop-ipv6-address</i>] <i>next-hop-ipv6-address</i> [... <i>default-next-hop-ipv6-address</i>]}
Mode	Route Map Configuration

Parameter	Description
<i>unit/slot/port</i>	If the IPv6 address is a link-local address, specify a routing interface (or VLAN ID).
<i>vlan-id</i>	If the IPv6 address is a link-local address, specify a VLAN ID in the range from 1 to 4093 (or an interface).
<i>default-next-hop-ipv6-address</i>	The global IPv6 address of the default next-hop router to which packets are routed. This address must be the address of an adjacent router. You can specify up to four IPv6 addresses. However, if you use the interface or interface vlan option, you can optionally specify one IPv6 address for a default next-hop router.

Usage guidelines

A packet is routed to the next-hop IPv6 address that is specified by the **set ipv6 default next-hop** command only if no explicit route for the packet destination address exists in the routing table. A default route in the routing table is not considered an explicit route for an unknown destination address.

In a route-map statement, the **set ipv6 next-hop** and **set ipv6 default next-hop** commands are mutually exclusive. However, you can configure the **set ipv6 default next-hop** command in a separate route-map statement.

When you configure the **set ipv6 default next-hop** command in a route map and apply it to an interface when a default route is also present on the switch, packets that match the route-map rules are routed according to the route map. This occurs because a default route is not considered an explicit route to a destination.

Command example:

```
(NETGEAR Switch) (Config) #route-map RouteMapName
(NETGEAR Switch) (route-map) #set ipv6 default next-hop 2002::2
```

no set ipv6 next-hop

Use this command to delete a default next-hop match statement from a route map.

Format	no set ipv6 default next-hop {interface {unit/slot/port vlan vlan-id} [...default-next-hop-ipv6-address] next-hop-ipv6-address [...default-next-hop-ipv6-address]}

Mode	Route Map Configuration

set ipv6 precedence

M4250

M4350

Use this command to set the three IP precedence bits in the IP packet header. With three bits, you have eight possible values for the IP precedence; *value* can be a number from 0 through 7. This command is used when implementing QoS and can be used by other QoS services, such as weighted fair queuing (WFQ) and weighted random early detection (WRED).

Default	No match criteria are defined by default.

Format	set ipv6 precedence <i>value</i>

Mode	Route Map Configuration

Parameter	Description
0	Sets the routine precedence
1	Sets the priority precedence
2	Sets the immediate precedence
3	Sets the Flash precedence
4	Sets the Flash override precedence
5	Sets the critical precedence
6	Sets the internetwork control precedence
7	Sets the network control precedence

no set ipv6 precedence

Use this command to reset the three IP precedence bits in the IP packet header to the default. By default, no match criteria are defined.

Format	no set ipv6 precedence

Mode	Route Map Configuration

OSPFv3 Commands

Note: Open Shortest Path First version 3 (OSPFv3) commands are supported on the M4350 series switches only. The M4250 series switches do not support OSPFv3.

This section describes the commands you use to configure OSPFv3, which is a link-state routing protocol that you use to route traffic within a network. This section includes the following subsections:

- [Global OSPFv3 Commands on page 1198](#)
- [OSPFv3 Interface Commands on page 1216](#)
- [OSPFv3 Graceful Restart Commands on page 1222](#)
- [OSPFv3 Stub Router Commands on page 1225](#)
- [OSPFv3 Show Commands on page 1227](#)

Global OSPFv3 Commands

Note: Open Shortest Path First version 3 (OSPFv3) commands are supported on the M4350 series switches only. The M4250 series switches do not support OSPFv3.

ipv6 router ospf

M4350

Use this command to enable ISPFv3 and let the CLI enter Router OSPFv3 Config mode.

Format	ipv6 router ospf

Mode	Global Config

no ipv6 router ospf

This command disables OSPFv3.

Format	no ipv6 router ospf

Mode	Global Config

area default-cost (Router OSPFv3 Config)

M4350

This command configures the metric default cost for the stub area. For the *value* argument, you must specify an integer value between 1–16777215.

Format	area <i>area-id</i> default-cost <i>value</i>

Mode	Router OSPFv3 Config

no ipv6 area default-cost (Router OSPFv3 Config)

This command resets the metric default cost for the stub area

Format	no ipv6 area <i>area-id</i> default-cost

Mode	Global Config

area nssa (Router OSPFv3 Config)

M4350

This command configures the specified *area-id* to function as an NSSA.

Format	<code>area area-id nssa</code>
Mode	Router OSPFv3 Config

no area nssa (Router OSPFv3 Config)

This command disables NSSA from the specified area id.

Format	<code>no area area-id nssa</code>
Mode	Router OSPFv3 Config

area nssa default-info-originate (Router OSPFv3 Config)

M4350

This command configures the metric value and type for the default route advertised into the NSSA. The optional *metric* parameter specifies the metric of the default route and must be in the range of 1–16777214. If no metric is specified, the default value is 10. The metric type can be comparable (nssa-external 1) or noncomparable (nssa-external 2).

Format	<code>area area-id nssa default-info-originate [metric] [comparable non-comparable]</code>
Mode	Router OSPFv3 Config

no area nssa default-info-originate (Router OSPFv3 Config)

This command disables the default route advertised into the NSSA.

Format	<code>no area area-id nssa default-info-originate [metric] [comparable non-comparable]</code>
Mode	Router OSPFv3 Config

area nssa no-redistribute (Router OSPFv3 Config)

M4350

This command configures the NSSA ABR so that learned external routes will not be redistributed to the NSSA.

Format	<code>area area-id nssa no-redistribute</code>
Mode	Router OSPFv3 Config

no area nssa no-redistribute (Router OSPFv3 Config)

This command disables the NSSA ABR so that learned external routes are redistributed to the NSSA.

Format	no area <i>area-id</i> nssa no-redistribute

Mode	Router OSPFv3 Config

area nssa no-summary (Router OSPFv3 Config)

M4350

This command configures the NSSA so that summary LSAs are not advertised into the NSSA.

Format	area <i>area-id</i> nssa no-summary

Mode	Router OSPFv3 Config

no area nssa no-summary (Router OSPFv3 Config)

This command disables NSSA from the summary LSAs.

Format	no area <i>area-id</i> nssa no-summary

Mode	Router OSPFv3 Config

area nssa translator-role (Router OSPFv3 Config)

M4350

This command configures the translator role of the NSSA. Selecting **always** causes the router to assume the role of the translator the instant it becomes a border router and selecting **candidate** causes the router to participate in the translator election process when it attains border router status.

Format	area <i>area-id</i> nssa translator-role {always candidate}

Mode	Router OSPFv3 Config

no area nssa translator-role (Router OSPFv3 Config)

This command disables the NSSA translator role from the specified area id.

Format	no area <i>area-id</i> nssa translator-role {always candidate}

Mode	Router OSPFv3 Config

area nssa translator-stab-intv (Router OSPFv3 Config)

M4350

This command configures the translator stability interval of the NSSA. The stability interval is the period that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another switch or router.

Format	<code>area area-id nssa translator-stab-intv stabilityinterval</code>
Mode	Router OSPFv3 Config

no area nssa translator-stab-intv (Router OSPFv3 Config)

This command disables the NSSA translator's stability interval from the specified area id.

Format	<code>no area area-id nssa translator-stab-intv stabilityinterval</code>
Mode	Router OSPFv3 Config

area range (Router OSPFv3 Config)

M4350

Use this command to configure an IPv6 prefix address and prefix length that an area border router advertises for a specific area.

Default	No area ranges are configured by default. No cost is configured by default.
Format	<code>area area-id range ipv6-prefix/prefix-length {summarylink nssaexternallink} [advertise not-advertise] [cost cost]</code>
Mode	Router OSPFv3 Config

Parameter	Description
area-id	The area identifier for the area whose networks are to be summarized.
ipv6-prefix/ prefix-length	The IPv6 prefix address and prefix length to be advertised when the ABR computes a route to one or more networks within this prefix in this area.
summarylink	The area range is used when summarizing prefixes advertised in type 3 summary LSAs.
nssaexternallink	The area range is used when translating type 7 LSAs to type 5 LSAs.
advertise	[Optional] The summary prefix is advertised when the area range is active. This is the default.
not-advertise	[Optional] Neither the summary prefix nor the contained prefixes are advertised when the area range is active. Any static cost previously configured is removed from the system configuration.
cost	[Optional] OSPF sets the metric field in the inter-area -prefix LSA to the configured value rather than setting the metric to the largest cost among the networks covered by the area range.

no area range (Router OSPFv3 Config)

The **no area range** command deletes a summary prefix or removes a static cost.

Format	<code>no area <i>area-id</i> range <i>ipv6-prefix/prefix-length</i> {summarylink nssaexternallink} cost</code>

Mode	Router OSPFv3 Config

area stub (Router OSPFv3 Config)

M4350

This command creates a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area.

Format	<code>area <i>area-id</i> stub</code>

Mode	Router OSPFv3 Config

no area stub (Router OSPFv3 Config)

This command deletes a stub area for the specified area ID.

Format	<code>no area <i>area-id</i> stub</code>

Mode	Router OSPFv3 Config

area stub no-summary (Router OSPFv3 Config)

M4350

This command disables the import of Summary LSAs for the stub area identified by *area-id*.

Default	enabled

Format	<code>area <i>area-id</i> stub no-summary</code>

Mode	Router OSPFv3 Config

no area stub no-summary (Router OSPFv3 Config)

This command sets the Summary LSA import mode to the default for the stub area identified by *area-id*.

Format	<code>no area <i>area-id</i> stub summarylsa</code>

Mode	Router OSPFv3 Config

area virtual-link (Router OSPFv3 Config)

M4350

This command creates the OSPF virtual interface for the specified *area-id* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Format	<i>area area-id virtual-link neighbor</i>

Mode	Router OSPFv3 Config

no area virtual-link (Router OSPFv3 Config)

This command deletes the OSPF virtual interface for the specified *area-id* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Format	<i>no area area-id virtual-link neighbor</i>

Mode	Router OSPFv3 Config

area virtual-link dead-interval (Router OSPFv3 Config)

M4350

This command configures the dead interval for the OSPF virtual interface on the virtual interface identified by *area-id* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. The range for *seconds* is 1 to 65535.

Default	40

Format	<i>area area-id virtual-link neighbor dead-interval seconds</i>

Mode	Router OSPFv3 Config

no area virtual-link dead-interval (Router OSPFv3 Config)

This command configures the default dead interval for the OSPF virtual interface on the virtual interface identified by *area-id* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Format	<i>no area area-id virtual-link neighbor dead-interval</i>

Mode	Router OSPFv3 Config

area virtual-link hello-interval (Router OSPFv3 Config)

M4350

This command configures the hello interval for the OSPF virtual interface on the virtual interface identified by *area-id* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. The range for *seconds* is from 1 to 65535.

Default	10
Format	<code>area area-id virtual-link neighbor hello-interval seconds</code>
Mode	Router OSPFv3 Config

no area virtual-link hello-interval (Router OSPFv3 Config)

This command configures the default hello interval for the OSPF virtual interface on the virtual interface identified by *area-id* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Format	<code>no area area-id virtual-link neighbor hello-interval</code>
Mode	Router OSPFv3 Config

area virtual-link retransmit-interval (Router OSPFv3 Config)

M4350

This command configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by *area-id* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. The range for *seconds* is 0 to 3600.

Default	5
Format	<code>area area-id virtual-link neighbor retransmit-interval seconds</code>
Mode	Router OSPFv3 Config

no area virtual-link retransmit-interval (Router OSPFv3 Config)

This command configures the default retransmit interval for the OSPF virtual interface on the virtual interface identified by *area-id* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Format	<code>no area area-id virtual-link neighbor retransmit-interval</code>
Mode	Router OSPFv3 Config

area virtual-link transmit-delay (Router OSPFv3 Config)

M4350

This command configures the transmit delay for the OSPF virtual interface on the virtual interface identified by *area-id* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. The range for *seconds* is 0 to 3600 (1 hour).

Default	1
Format	<code>area area-id virtual-link neighbor transmit-delay seconds</code>
Mode	Router OSPFv3 Config

no area virtual-link transmit-delay (Router OSPFv3 Config)

This command configures the default transmit delay for the OSPF virtual interface on the virtual interface identified by *area-id* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Format	<code>no area area-id virtual-link neighbor transmit-delay</code>
Mode	Router OSPFv3 Config

auto-cost (Router OSPFv3 Config)

M4350

By default, OSPF computes the link cost of each interface from the interface bandwidth. Faster links have lower metrics, making them more attractive in route selection. The configuration parameters in the **auto-cost reference bandwidth** and **bandwidth** commands give you control over the default link cost. You can configure for OSPF an interface bandwidth that is independent of the actual link speed. A second configuration parameter allows you to control the ratio of interface bandwidth to link cost. The link cost is computed as the ratio of a reference bandwidth to the interface bandwidth ($\text{ref\_bw} / \text{interface bandwidth}$), where interface bandwidth is defined by the **bandwidth** command. Because the default reference bandwidth is 100 Mbps, OSPF uses the same default link cost for all interfaces whose bandwidth is 100 Mbps or greater. Use the **auto-cost reference-bandwidth** command to change the reference bandwidth, specifying the reference bandwidth in megabits per second (Mbps). For the *mbps* variable, the reference bandwidth range is 1–4294967 Mbps.

Default	100 Mbps
Format	<code>auto-cost reference-bandwidth mbps</code>
Mode	Router OSPFv3 Config

no auto-cost reference-bandwidth (Router OSPFv3 Config)

Use this command to set the reference bandwidth to the default value.

Format	<code>no auto-cost reference-bandwidth</code>
Mode	Router OSPFv3 Config

clear ipv6 ospf

M4350

Use this command to disable and re-enable OSPF.

Format	<code>clear ipv6 ospf</code>
Mode	Privileged EXEC

clear ipv6 ospf configuration

M4350

Use this command to reset the OSPF configuration to factory defaults.

Format	<code>clear ipv6 ospf configuration</code>
Mode	Privileged EXEC

clear ipv6 ospf counters

M4350

Use this command to reset global and interface statistics.

Format	<code>clear ipv6 ospf counters</code>
Mode	Privileged EXEC

clear ipv6 ospf neighbor

M4350

Use this command to drop the adjacency with all OSPF neighbors. On each neighbor's interface, send a one-way hello. Adjacencies may then be re-established. To drop all adjacencies with a specific router ID, specify the neighbor's Router ID using the optional parameter *neighbor-id*.

Format	<code>clear ipv6 ospf neighbor [<i>neighbor-id</i>]</code>
Mode	Privileged EXEC

clear ipv6 ospf neighbor interface

M4350

To drop adjacency with all neighbors on a specific interface, use the optional parameter *unit/slot/port*.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

To drop adjacency with a specific router ID on a specific interface, use the optional parameter *neighbor-id*.

Format	<code>clear ipv6 ospf neighbor interface [unit/slot/port vlan vlan-id] [neighbor-id]</code>

Mode	Privileged EXEC

clear ipv6 ospf redistribution

M4350

Use this command to flush all self-originated external LSAs. Reapply the redistribution configuration and re-originate prefixes as necessary.

Format	<code>clear ipv6 ospf redistribution</code>

Mode	Privileged EXEC

default-information originate (Router OSPFv3 Config)

M4350

This command is used to control the advertisement of default routes. The *metric* argument can be a number in the range 0–16777214. The metric type can be 1 or 2.

Default	<i>metric</i> —unspecified <i>type</i> —2

Format	<code>default-information originate [always] [metric metric] [metric-type {1 2}]</code>

Mode	Router OSPFv3 Config

no default-information originate (Router OSPFv3 Config)

This command is used to control the advertisement of default routes.

Format	<code>no default-information originate [metric] [metric-type]</code>

Mode	Router OSPFv3 Config

default-metric (Router OSPFv3 Config)

M4350

This command is used to set a default for the metric of distributed routes. The *metric* argument can be a number in the range 0–16777214.

Format	default-metric <i>metric</i>

Mode	Router OSPFv3 Config

no default-metric (Router OSPFv3 Config)

This command is used to set a default for the metric of distributed routes.

Format	no default-metric

Mode	Router OSPFv3 Config

distance ospf (Router OSPFv3 Config)

M4350

This command sets the route preference value of OSPF route types in the router. Lower route preference values are preferred when determining the best route. The type of OSPF route can be intra, inter, or external. All the external type routes are given the same preference value. The range for the *preference* value is from 1 to 255.

Default	110

Format	distance ospf {intra-area <i>preference</i> inter-area <i>preference</i> external <i>preference</i> }

Mode	Router OSPFv3 Config

no distance ospf (Router OSPFv3 Config)

This command sets the default route preference value of OSPF routes in the router. The type of OSPF route can be intra, inter, or external. All the external type routes are given the same preference value.

Format	no distance ospf {intra-area inter-area external}

Mode	Router OSPFv3 Config

enable (Router OSPFv3 Config)

M4350

This command resets the administrative mode of OSPF on the switch to active.

Default	enabled
Format	enable
Mode	Router OSPFv3 Config

no enable (Router OSPFv3 Config)

This command sets the administrative mode of OSPF in the router to inactive.

Format	no enable
Mode	Router OSPFv3 Config

exit-overflow-interval (Router OSPFv3 Config)

M4350

This command configures the exit overflow interval for OSPF. It describes the number of seconds after entering Overflow state that a router will wait before attempting to leave the overflow state. This allows the router to again originate nondefault AS-external-LSAs. When set to 0, the router does not leave overflow state until restarted. The range for *seconds* is from 0 to 2147483647 seconds.

Default	0
Format	exit-overflow-interval <i>seconds</i>
Mode	Router OSPFv3 Config

no exit-overflow-interval (Router OSPFv3 Config)

This command configures the default exit overflow interval for OSPF.

Format	no exit-overflow-interval
Mode	Router OSPFv3 Config

external-lsdb-limit (Router OSPFv3 Config)

M4350

This command configures 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 nondefault AS-external-LSAs in its 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 *limit* is from -1 to 2147483647.

Default	-1
Format	<code>external-lsdb-limit limit</code>
Mode	Router OSPFv3 Config

no external-lsdb-limit (Router OSPFv3 Config)

This command configures the default external LSDB limit for OSPF.

Format	<code>no external-lsdb-limit</code>
Mode	Router OSPFv3 Config

maximum-paths (Router OSPFv3 Config)

M4350

This command sets the number of paths that OSPF can report for a destination where *maxpaths* is platform dependent.

Default	4
Format	<code>maximum-paths maxpaths</code>
Mode	Router OSPFv3 Config

no maximum-paths (Router OSPFv3 Config)

This command resets the number of paths that OSPF can report for a destination back to its default value.

Format	<code>no maximum-paths</code>
Mode	Router OSPFv3 Config

passive-interface default (Router OSPFv3 Config)

M4350

Use this command to enable global passive mode by default for all interfaces, which overrides any interface-level passive mode. OSPF does not form adjacencies over a passive interface.

Default	disabled
Format	<code>passive-interface default</code>
Mode	Router OSPFv3 Config

no passive-interface default (Router OSPFv3 Config)

Use this command to disable the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to non-passive mode.

Format	no passive-interface default

Mode	Router OSPFv3 Config

passive-interface (Router OSPFv3 Config)

M4350

Use this command to set the interface as passive.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

Using these arguments overrides the global passive mode that is effective on the interface or VLAN.

Default	disabled

Format	passive-interface { <i>unit/slot/port</i> <i>vlan vlan-id</i> }

Mode	Router OSPFv3 Config

no passive-interface (Router OSPFv3 Config)

Use this command to set the interface or VLAN as non-passive. It overrides the global passive mode that is currently effective on the interface or VLAN.

Format	no passive-interface { <i>unit/slot/port</i> <i>vlan vlan-id</i> }

Mode	Router OSPFv3 Config

prefix-suppression (Router OSPFv3 Config)

M4350

This command suppresses the advertisement of all the IPv6 prefixes except for prefixes that are associated with secondary IPv6 addresses, loopbacks, and passive interfaces from the OSPFv3 router advertisements.

To suppress a loopback or passive interface, use the **ipv ospf prefix-suppression** command in interface configuration mode. Prefixes associated with secondary IPv6 addresses can never be suppressed.

Default	Prefix suppression is disabled.
Format	<code>prefix-suppression</code>
Mode	Router OSPFv3 Config

`no prefix-suppression` (Router OSPFv3 Config)

This command disables prefix-suppression. No prefixes are suppressed from getting advertised.

Format	<code>no prefix-suppression</code>
Mode	Router OSPFv3 Config

`redistribute` (Router OSPFv3 Config)

M4350

This command configures the OSPFv3 protocol to allow redistribution of static or connected routes. The *metric* argument is in the range from 0 to 16777214. For the **metric type** keyword, you can select 1 or 2. The *tag* argument can be from 0 to 4294967295.

Default	metric: not specified type: 2 tag: 0
Format	<code>redistribute {static connected} [metric <i>metric</i>] [metric-type {1 2}] [tag <i>tag</i>]</code>
Mode	Router OSPFv3 Config

Command example:

```
(NETGEAR Switch) (Config)#ipv6 router ospf
(NETGEAR Switch) (Config-rtr)#redistribute connected metric 165543 metric-type 2 tag
3680012
```

`no redistribute` (Router OSPFv3 Config)

This command disables the OSPF protocol from redistributing static or connected routes.

Format	<code>no redistribute {static connected} [metric] [metric-type] [tag]</code>
Mode	Router OSPFv3 Config

router-id (Router OSPFv3 Config)

M4350

This command sets a 4-digit dotted-decimal number uniquely identifying the router OSPF ID. The *ipaddress* is a configured value.

Format	<code>router-id ipaddress</code>

Mode	Router OSPFv3 Config

no router-id (Router OSPFv3 Config)

This command resets the router OSPF ID.

Format	<code>no router-id</code>

Mode	Router OSPFv3 Config

timers pacing lsa-group (Router OSPFv3 Config)

M4350

Use this command to adjust how OSPFv3 groups LSAs for periodic refresh. OSPFv3 refreshes self-originated LSAs approximately once every 30 minutes. When OSPFv3 refreshes LSAs, it considers all self-originated LSAs whose age is from 1800 to 1800 plus the pacing group size. Grouping LSAs for refresh allows OSPFv3 to combine refreshed LSAs into a minimal number of LS Update packets. Minimizing the number of Update packets makes LSA distribution more efficient.

When OSPFv3 originates a new or changed LSA, it selects a random refresh delay for the LSA. When the refresh delay expires, OSPFv3 refreshes the LSA. By selecting a random refresh delay, OSPFv3 avoids refreshing a large number of LSAs at one time, even if a large number of LSAs are originated at one time.

The *seconds* argument represents the width of the window in which LSAs are refreshed. For the *seconds* argument, the range for the pacing group window is from 10 to 1800 seconds.

Default	60 seconds

Format	<code>timers pacing lsa-group seconds</code>

Mode	Router OSPFv3 Config

no timers pacing lsa-group (Router OSPFv3 Config)

This command returns the LSA Group Pacing parameter to the factory default value of 60 seconds.

Format	<code>no timers pacing lsa-group</code>

Mode	Router OSPFv3 Config

timers throttle spf (Router OSPFv3 Config)

M4350

The initial wait interval is set to an amount of delay specified by the *spf-hold* value. If an SPF calculation is not scheduled during the current wait interval, the next SPF calculation is scheduled at a delay of *spf-start*. If there has been an SPF calculation scheduled during the current wait interval, the wait interval is set to two times the current wait interval until the wait interval reaches the maximum time in milliseconds as specified in *spf-maximum*. Subsequent wait times remain at the maximum until the values are reset or an LSA is received between SPF calculations.

Default	<i>spf-start</i> = 2000 ms <i>spf-hold</i> = 5000 ms <i>spf-maximum</i> = 5000 ms
Format	<code>timers throttle spf spf-start spf-hold spf-maximum</code>
Mode	Router OSPFv3 Config
Parameter	Description
<i>spf-start</i>	Indicates the SPF schedule delay in milliseconds when no SPF calculation has been scheduled during the current wait interval. Value range is 1 to 600000 milliseconds.
<i>spf-hold</i>	Indicates the initial SPF wait interval in milliseconds. Value range is 1 to 600000 milliseconds.
<i>spf-maximum</i>	Indicates the maximum SPF wait interval in milliseconds. Value range is 1 to 600000 milliseconds.

no timers throttle spf (Router OSPFv3 Config)

This command returns the SPF throttling parameters to the factory default values.

Format	<code>no timers throttle spf</code>
Mode	Router OSPFv3 Config

trapflags (Router OSPFv3 Config)

M4350

Use this command to enable individual OSPF traps, enable a group of trap flags at a time, or enable all the trap flags at a time. The different groups of trap flags, and each group's specific trap flags to enable or disable, are listed in the following table.

Table 11. Trap flag groups (OSPFv3)

Group	Flags
errors	• authentication-failure • bad-packet • config-error • virt-authentication-failure • virt-bad-packet • virt-config-error
lsa	• lsa-maxage • lsa-originate
overflow	• lsdb-overflow • lsdb-approaching-overflow
retransmit	• packets • virt-packets
state-change	• if-state-change • neighbor-state-change • virtif-state-change • virtneighbor-state-change

- To enable an individual flag, enter the **trapflags group name** followed by a particular flag.
- To enable all the flags in that group, enter **trapflags group name** followed by **all**.
- To enable all the flags, enter the command as **trapflags all**.

Default	disabled
Format	<pre>trapflags {all errors {all authentication-failure bad-packet config-error virt-authentication-failure virt-bad-packet virt-config-error} lsa {all lsa-maxage lsa-originate} overflow {all lsdb-overflow lsdb-approaching-overflow} retransmit {all packets virt-packets} state-change {all if-state-change neighbor-state-change virtif-state-change virtneighbor-state-change}}</pre>
Mode	Router OSPFv3 Config

no trapflags (Router OSPFv3 Config)

Use this command to revert to the default trap flag settings, in which all trap flags are disabled.

- To disable an individual flag, enter the **no trapflags group name** followed by a particular flag.
- To disable all the flags in that group, enter **no trapflags group name** followed by **all**.
- To disable all the flags, enter the command as **no trapflags all**.

Format	no trapflags {all errors {all authentication-failure bad-packet config-error virt-authentication-failure virt-bad-packet virt-config-error} lsa {all lsa-maxage lsa-originate} overflow {all lsdbs-overflow lsdbs-approaching-overflow} retransmit {all packets virt-packets} state-change {all if-state-change neighbor-state-change virtif-state-change virtneighbor-state-change}}

Mode	Router OSPFv3 Config

OSPFv3 Interface Commands

Note: Open Shortest Path First version 3 (OSPFv3) commands are supported on the M4350 series switches only. The M4250 series switches do not support OSPFv3.

ipv6 ospf area

M4350

This command sets the OSPF area to which the specified router interface or range of interfaces belongs. It also enables OSPF on the specified router interface or range of interfaces.

The *area-id* is a 32-bit integer, formatted either as a 4-digit dotted-decimal number or a decimal value in the range of 0-4294967295. The *area-id* uniquely identifies the area to which the interface connects. Assigning an area ID for an area that does not yet exist, causes the area to be created with default values.

Format	ipv6 ospf area <i>area-id</i>

Mode	Interface Config

ipv6 ospf cost

M4350

This command configures the cost on an OSPF interface or range of interfaces. The *cost* parameter is in the range of 1 to 65535.

Default	10
Format	ipv6 ospf cost <i>cost</i>
Mode	Interface Config

no ipv6 ospf cost

This command configures the default cost on an OSPF interface.

Format	no ipv6 ospf cost
Mode	Interface Config

ipv6 ospf dead-interval

M4350

This command sets the OSPF dead interval for the specified interface or range of interfaces. The value for *seconds* is a valid positive integer, which represents the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (that is, 4). A valid value for *seconds* is in the range from 1-65535.

Default	40
Format	ipv6 ospf dead-interval <i>seconds</i>
Mode	Interface Config

no ipv6 ospf dead-interval

This command sets the default OSPF dead interval for the specified interface or range of interfaces.

Format	no ipv6 ospf dead-interval
Mode	Interface Config

ipv6 ospf hello-interval

M4350

This command sets the OSPF hello interval for the specified interface. The value for *seconds* is a valid positive integer, which represents the length of time in seconds. The

value for the length of time must be the same for all routers attached to a network. A valid value for *seconds* is in the range from 1 to 65535.

Default	10
Format	<code>ipv6 ospf hello-interval seconds</code>
Mode	Interface Config

`no ipv6 ospf hello-interval`

This command sets the default OSPF hello interval for the specified interface.

Format	<code>no ipv6 ospf hello-interval</code>
Mode	Interface Config

ipv6 ospf link-lsa-suppression

M4350

Use this command to enable Link LSA Suppression on an interface. When Link LSA Suppression is enabled on a point-to-point (P2P) interface, no Link LSA protocol packets are originated (transmitted) on the interface. This configuration does not apply to non-P2P interfaces.

Default	False
Format	<code>ipv6 ospf link-lsa-suppression</code>
Mode	Privileged EXEC

`no ipv6 ospf link-lsa-suppression`

This command returns Link LSA Suppression for the interface to disabled. When Link LSA Suppression is disabled, Link LSA protocol packets are originated (transmitted) on the P2P interface.

Format	<code>no ipv6 ospf link-lsa-suppression</code>
Mode	Privileged EXEC

ipv6 ospf mtu-ignore

M4350

This command disables OSPF maximum transmission unit (MTU) mismatch detection on an interface or range of interfaces. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By

default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

Default	enabled
Format	<code>ipv6 ospf mtu-ignore</code>
Mode	Interface Config

`no ipv6 ospf mtu-ignore`

This command enables the OSPF MTU mismatch detection.

Format	<code>no ipv6 ospf mtu-ignore</code>
Mode	Interface Config

`ipv6 ospf network`

M4350

This command changes the default OSPF network type for the interface or range of interfaces. Normally, the network type is determined from the physical IP network type. By default, all Ethernet networks are OSPF type broadcast. When an Ethernet port is used as a single large bandwidth IP network between two routers, the network type can be point-to-point since there are only two routers.

Using point-to-point as the network type eliminates the overhead of the OSPF designated router election.

Default	broadcast
Format	<code>ipv6 ospf network {broadcast point-to-point}</code>
Mode	Interface Config

`no ipv6 ospf network`

This command sets the interface type to the default value.

Format	<code>no ipv6 ospf network {broadcast point-to-point}</code>
Mode	Interface Config

`ipv6 ospf prefix-suppression`

M4350

This command suppresses the advertisement of the IPv6 prefixes that are associated with an interface, except for those associated with secondary IPv6 addresses. This command takes precedence over the global configuration. If this configuration is not specified, the global prefix-suppression configuration applies.

prefix-suppression can be disabled at the interface level by using the `disable` option. The `disable` option is useful for excluding specific interfaces from performing prefix-suppression when the feature is enabled globally.

Note that the `disable` option `disable` is not equivalent to not configuring the interface specific prefix-suppression. If prefix-suppression is not configured at the interface level, the global prefix-suppression configuration is applicable for the IPv6 prefixes associated with the interface.

Default	prefix-suppression is not configured.
Format	<code>ipv6 ospf prefix-suppression [disable]</code>
Mode	Interface Config

`no ipv6 ospf prefix-suppression`

This command removes prefix-suppression configurations at the interface level. When the `no ipv6 ospf prefix-suppression` command is used, global prefix-suppression applies to the interface. However, entering the `no ipv6 ospf prefix-suppression` command is not the same as disabling interface level prefix-suppression.

Format	<code>no ipv6 ospf prefix-suppression</code>
Mode	Interface Config

`ipv6 ospf priority`

M4350

This command sets the OSPF priority for the specified router interface or range of interfaces. For the *priority* argument, the priority of the interface is an integer in the range from 0 to 255. A value of 0 indicates that the router is not eligible to become the designated router on this network.

Default	1, which is the highest router priority
Format	<code>ipv6 ospf priority <i>priority</i></code>
Mode	Interface Config

`no ipv6 ospf priority`

This command sets the default OSPF priority for the specified router interface.

Format	<code>no ipv6 ospf priority</code>
Mode	Interface Config

ipv6 ospf retransmit-interval

M4350

This command sets the OSPF retransmit Interval for the specified interface or range of interfaces. The retransmit interval is specified in seconds. The value for *seconds* is the number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. For the *seconds* argument, a valid value is in the range from 0 to 3600 seconds (1 hour).

Default	5
Format	ipv6 ospf retransmit-interval <i>seconds</i>
Mode	Interface Config

no ipv6 ospf retransmit-interval

This command sets the default OSPF retransmit Interval for the specified interface.

Format	no ipv6 ospf retransmit-interval
Mode	Interface Config

ipv6 ospf transmit-delay

M4350

This command sets the OSPF transmit delay for the specified interface or range of interfaces. The transmit delay is specified in seconds. In addition, it sets the estimated number of seconds it takes to transmit a link state update packet over this interface. For the *seconds* argument, a valid value is in the range from 0 to 3600 seconds (1 hour).

Default	1
Format	ipv6 ospf transmit-delay <i>seconds</i>
Mode	Interface Config

no ipv6 ospf transmit-delay

This command sets the default OSPF transmit delay for the specified interface.

Format	no ipv6 ospf transmit-delay
Mode	Interface Config

OSPFv3 Graceful Restart Commands

Note: Open Shortest Path First version 3 (OSPFv3) commands are supported on the M4350 series switches only. The M4250 series switches do not support OSPFv3.

The OSPFv3 protocol can be configured to participate in the check-pointing service, so that these protocols can execute a graceful restart when the management unit fails. In a graceful restart, the hardware continues forwarding IPv6 packets using OSPFv3 routes while a backup switch takes over management unit responsibility.

Graceful restart uses the concept of helpful neighbors. A fully adjacent router enters helper mode when it receives a link state announcement (LSA) from the restarting management unit indicating its intention of performing a graceful restart. In helper mode, a switch continues to advertise to the rest of the network that they have full adjacencies with the restarting router, thereby avoiding announcement of a topology change and the potential for flooding of LSAs and shortest-path-first (SPF) runs (which determine OSPF routes). Helpful neighbors continue to forward packets through the restarting router. The restarting router relearns the network topology from its helpful neighbors.

Graceful restart can be enabled for either planned or unplanned restarts, or both. You can initiate a planned restart through the management command **initiate failover**. You can initiate a failover in order to take the management unit out of service (for example, to address a partial hardware failure), to correct faulty system behavior which cannot be corrected through less severe management actions, or other reasons. An unplanned restart is an unexpected failover caused by a fatal hardware failure of the management unit or a software hang or crash on the management unit.

nsf (Router OSPFv3 Config)

M4350

Use this command to enable the OSPF graceful restart functionality on an interface. To disable graceful restart, use the no form of the command.

Default	Disabled
Format	nsf [ietf] [planned-only]
Modes	Router OSPFv3 Config

Parameter	Description
ietf	This keyword is accepted but not required.
planned-only	This optional keyword indicates that OSPF should only perform a graceful restart when the restart is planned (that is, when the restart is a result of the initiate failover command).

no nsf (Router OSPFv3 Config)

Use this command to disable graceful restart for all restarts.

Format	no nsf [ietf] [planned-only]

Modes	Router OSPFv3 Config

nsf restart-interval (Router OSPFv3 Config)

M4350

Use this command to configure the number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. This is referred to as the grace period. The restarting router includes the grace period in its grace LSAs. For planned restarts (using the **initiate failover** command), the grace LSAs are sent prior to restarting the management unit, whereas for unplanned restarts, they are sent after reboot begins.

The grace period must be set long enough to allow the restarting router to reestablish all of its adjacencies and complete a full database exchange with each of those neighbors. For the *seconds* argument, a valid value is in the range from 0 to 1800 seconds.

Default	120 seconds

Format	nsf [ietf] restart-interval <i>seconds</i>

Modes	Router OSPFv3 Config

Parameter	Description
ietf	This keyword is accepted but not required.
seconds	The number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. The range is from 1 to 1800 seconds.

no nsf restart-interval (Router OSPFv3 Config)

Use this command to revert the grace period to its default value.

Format	no [ietf] nsf restart-interval

Modes	Router OSPFv3 Config

nsf helper (Router OSPFv3 Config)

M4350

Use this command to enable helpful neighbor functionality for the OSPF protocol. You can enable this functionality for planned or unplanned restarts, or both.

Default	OSPF may act as a helpful neighbor for both planned and unplanned restarts
Format	<code>nsf helper [planned-only]</code>
Modes	Router OSPFv3 Config

Parameter	Description
planned-only	This optional keyword indicates that OSPF should only help a restarting router performing a planned restart.

no nsf helper (Router OSPFv3 Config)

Use this command to disable helpful neighbor functionality for OSPF.

Format	<code>no nsf helper</code>
Modes	Router OSPFv3 Config

nsf ietf helper disable (Router OSPFv3 Config)

M4350

Use this command to disable helpful neighbor functionality for OSPF.

Note: The commands `no nsf helper` and `nsf ietf helper disable` are functionally equivalent. The command `nsf ietf helper disable` is supported solely for compatibility with other network software CLI.

Format	<code>nsf ietf helper disable</code>
Modes	Router OSPFv3 Config

nsf helper strict-lsa-checking (Router OSPFv3 Config)

M4350

The restarting router is unable to react to topology changes. In particular, the restarting router will not immediately update its forwarding table; therefore, a topology change may introduce forwarding loops or black holes that persist until the graceful restart completes. By exiting the graceful restart on a topology change, a router tries to eliminate the loops or black holes as

quickly as possible by routing around the restarting router. A helpful neighbor considers a link down with the restarting router to be a topology change, regardless of the strict LSA checking configuration.

Use this command to require that an OSPF helpful neighbor exit helper mode whenever a topology change occurs.

Default	Enabled.
Format	<code>nsf [ietf] helper strict-lsa-checking</code>
Modes	Router OSPFv3 Config
Parameter	Description
ietf	This keyword is accepted but not required.

`no nsf helper strict-lsa-checking` (Router OSPFv3 Config)

Use this command to allow OSPF to continue as a helpful neighbor in spite of topology changes.

Default	Enabled.
Format	<code>nsf [ietf] helper strict-lsa-checking</code>
Modes	Router OSPFv3 Config

OSPFv3 Stub Router Commands

Note: Open Shortest Path First version 3 (OSPFv3) commands are supported on the M4350 series switches only. The M4250 series switches do not support OSPFv3.

`max-metric router-lsa` (OSPFv3 Router Configuration)

M4350

To configure OSPFv3 to enter stub router mode, use this command in Router OSPFv3 Global Configuration mode. When OSPFv3 is in stub router mode, OSPFv3 sets the metric in the nonstub links in its router LSA to MaxLinkMetric. Other switches or routers therefore compute very long paths through the stub router, and prefer any alternate path. Doing so eliminates all transit traffic through the stub router, when alternate routes are available. Stub router mode is useful when adding or removing a router from a network or to avoid transient routes when a router reloads.

You can administratively force OSPFv3 into stub router mode. OSPFv3 remains in stub router mode until you take OSPFv3 out of stub router mode. Alternatively, you can configure OSPF to start in stub router mode for a configurable period of time after the router boots up.

If you set the summary LSA metric to 16,777,215, other routers skip the summary LSA when they compute routes.

If you have configured the switch or router to enter stub router mode on startup (using the **max-metric router-lsa on-startup** command), and then enter the **max-metric router-lsa** command, there is no change. If OSPFv3 is administratively in stub router mode (that is, you have entered the **max-metric router-lsa** command), and you configure OSPFv3 to enter stub router mode on startup (using the **max-metric router-lsa on-startup** command), OSPFv3 exits stub router mode (assuming the startup period has expired) and the configuration is updated. Without any parameters, stub router mode only sends maximum metric values for router LSAs.

Default	OSPF is not in stub router mode by default
Format	<code>max-metric router-lsa [external-lsa <i>metric</i>] [inter-area-lsas <i>metric</i>] [on-startup <i>seconds</i>] [summary-lsa <i>metric</i>]</code>
Mode	OSPFv3 Router Configuration

Parameter	Description
external-lsa	(Optional) Sends the maximum metric values for external LSAs. The <i>metric</i> argument is the maximum metric value to use for LSAs. The range is 1 to 16777215 (0xFFFFFFFF). The default value is 16711680 (0xFF0000).
inter-area-lsas	(Optional) Sends the maximum metric values for Inter-Area-Router LSAs. The <i>metric</i> argument is the maximum metric value to use for LSAs. The range is 1 to 16777215 (0xFFFFFFFF). The default value is 16711680 (0xFF0000).
on-startup	(Optional) Starts OSPF in stub router mode. The <i>seconds</i> argument is the number of seconds that OSPF remains in stub router mode after a reboot. The range is 5 to 86,400 seconds. There is no default value.
summary-lsa	(Optional) Sends the maximum metric values for Summary LSAs. The <i>metric</i> argument is the maximum metric value to use for LSAs. The range is 1 to 16777215 (0xFFFFFFFF). The default value is 16711680 (0xFF0000).

no max-metric router-lsa (OSPFv3 Router Configuration)

Use this command in OSPFv3 Router Configuration mode to disable stub router mode. The command clears either type of stub router mode (always or on-startup) and resets all LSA options. If OSPF is configured to enter global configuration mode on startup, and during normal operation you want to immediately place OSPF in stub router mode, enter the **no max-metric router-lsa on-startup** command. The command **no max-metric router-lsa** with the **external-lsa**, **inter-area-lsas**, **on-startup**, or **summary-lsa** keyword causes OSPF to send summary LSAs with metrics computed using normal procedures.

Format	<code>no max-metric router-lsa [external-lsa] [inter-area-lsas] [on-startup] [summary-lsa]</code>

Mode	OSPFv3 Router Configuration

`clear ipv6 ospf stub-router`

M4350

Use this command to force OSPF to exit stub router mode when it has automatically entered stub router mode because of a resource limitation. OSPF only exits stub router mode if it entered stub router mode because of a resource limitation or if it is in stub router mode at startup. This command does not take effect if OSPF is configured to be in stub router mode permanently.

Format	<code>clear ipv6 ospf stub-router</code>

Mode	Privileged EXEC

OSPFv3 Show Commands

Note: Open Shortest Path First version 3 (OSPFv3) commands are supported on the M4350 series switches only. The M4250 series switches do not support OSPFv3.

`show ipv6 ospf`

M4350

This command displays information relevant to the OSPF router.

Format	<code>show ipv6 ospf</code>

Mode	Privileged EXEC User EXEC

Note: Some of the information below displays only if you enable OSPF and configure certain features.

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Router ID	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
OSPF Admin Mode	Shows whether the administrative mode of OSPF in the router is enabled or disabled. This is a configured value.
External LSDB Limit	The maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database.
Exit Overflow Interval	The number of seconds that, after entering overflow state, a router will attempt to leave overflow state.
SPF Start Time	The number of milliseconds the SPF calculation is delayed if no SPF calculation has been scheduled during the current "wait interval".
SPF Hold Time	The number of milliseconds of the initial wait interval.
SPF Maximum Hold Time	The maximum number of milliseconds of the "wait interval".
LSA Refresh Group Pacing Time	The size of the LSA refresh group window, in seconds.
AutoCost Ref BW	Shows the value of the auto-cost reference bandwidth configured on the router.
Default Passive Setting	Shows whether the interfaces are passive by default.
Maximum Paths	The maximum number of paths that OSPF can report for a destination.
Default Metric	Default value for redistributed routes.
Default Route Advertise	Indicates whether the default routes received from other source protocols are advertised or not.
Always	Shows whether default routes are always advertised.
Metric	The metric for the advertised default routes. If the metric is not configured, this field is blank.
Metric Type	Shows whether the routes are External Type 1 or External Type 2.
Number of Active Areas	The number of active OSPF areas. An active OSPF area is an area with at least one interface up.
ABR Status	Shows whether the router is an OSPF Area Border Router.
ASBR Status	Shows if 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 learnt from other protocol. The possible values for the ASBR status is enabled (if the router is configured to re-distribute routes learned by other protocols) or disabled (if the router is not configured for the same).
Stub Router Status	The status of the stub router: Active or Inactive.
Stub Router Reason	This is displayed only if the stub router is active. Shows the reason for the stub router: Configured, Startup, or Resource Limitation

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Stub Router Startup Time Remaining	This is displayed only if the stub router is in startup stub router mode. The remaining time (in seconds) until OSPF exits stub router mode.
Stub Router Duration	This row is only listed if the stub router is active and the router entered stub mode because of a resource limitation. The time elapsed since the router last entered the stub router mode. The duration is displayed in DD:HH:MM:SS format.
External LSDB Overflow	When the number of non-default external LSAs exceeds the configured limit, External LSDB Limit, OSPF goes into LSDB overflow state. In this state, OSPF withdraws all of its self-originated non-default external LSAs. After the Exit Overflow Interval, OSPF leaves the overflow state, if the number of external LSAs has been reduced.
External LSA Count	The number of external (LS type 5) link-state advertisements in the link-state database.
External LSA Checksum	The sum of the LS checksums of external link-state advertisements contained in the link-state database.
New LSAs Originated	The number of new link-state advertisements that have been originated.
LSAs Received	The number of link-state advertisements received determined to be new instantiations.
LSA Count	The total number of link state advertisements currently in the link state database.
Maximum Number of LSAs	The maximum number of LSAs that OSPF can store.
LSA High Water Mark	The maximum size of the link state database since the system started.
Retransmit List Entries	The total number of LSAs waiting to be acknowledged by all neighbors. An LSA may be pending acknowledgment from more than one neighbor.
Maximum Number of Retransmit Entries	The maximum number of LSAs that can be waiting for acknowledgment.
Retransmit Entries High Water Mark	The highest number of LSAs that have been waiting for acknowledgment.
Redistributing	This field is a heading and appears only if you configure the system to take routes learned from a non-OSPF source and advertise them to its peers.
Source	Shows source protocol/routes that are being redistributed. Possible values are static, connected, BGP, or RIP.
Metric	The metric of the routes being redistributed.
Metric Type	Shows whether the routes are External Type 1 or External Type 2.
Tag	The decimal value attached to each external route.
Subnets	For redistributing routes into OSPF, the scope of redistribution for the specified protocol.
Distribute-List	The access list used to filter redistributed routes.

Term	Definition
Prefix-suppression	Displays whether prefix-suppression is enabled or disabled on the specified interface.
NSF Support	Indicates whether nonstop forwarding (NSF) is enabled for the OSPF protocol for planned restarts, unplanned restarts or both (Always).
NSF Restart Interval	The user-configurable grace period during which a neighboring router will be in the helper state after receiving notice that the management unit is performing a graceful restart.
NSF Restart Status	The current graceful restart status of the router.
NSF Restart Age	Number of seconds until the graceful restart grace period expires.
NSF Restart Exit Reason	Indicates why the router last exited the last restart: • None. Graceful restart has not been attempted. • In Progress. Restart is in progress. • Completed. The previous graceful restart completed successfully. • Timed Out. The previous graceful restart timed out. • Topology Changed. The previous graceful restart terminated prematurely because of a topology change.
NSF Help Support	Indicates whether helpful neighbor functionality has been enabled for OSPF for planned restarts, unplanned restarts, or both (Always).
NSF help Strict LSA checking	Indicates whether strict LSA checking has been enabled. If enabled, then an OSPF helpful neighbor will exit helper mode whenever a topology change occurs. If disabled, an OSPF neighbor will continue as a helpful neighbor in spite of topology changes.

show ipv6 ospf abr

M4350

This command displays the internal OSPFv3 routes to reach Area Border Routers (ABR).

Format	<code>show ipv6 ospf abr</code>
Modes	Privileged EXEC User EXEC

Term	Definition
Type	The type of the route to the destination. It can be either: • intra — Intra-area route • inter — Inter-area route
Router ID	Router ID of the destination.
Cost	Cost of using this route.
Area ID	The area ID of the area from which this route is learned.
Next Hop	Next hop toward the destination.
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

show ipv6 ospf area

M4350

This command displays information about the area. The *area-id* identifies the OSPF area that is displayed.

Format	<code>show ipv6 ospf area area-id</code>
Modes	Privileged EXEC User EXEC
Term	Definition
AreaID	The area id of the requested OSPF area.
External Routing	A number representing the external routing capabilities for this area.
Spf Runs	The number of times that the intra-area route table has been calculated using this area's link-state database.
Area Border Router Count	The total number of area border routers reachable within this area.
Area LSA Count	Total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
Area LSA Checksum	A number representing the Area LSA Checksum for the specified area ID excluding the external (LS type 5) link-state advertisements.
Stub Mode	Represents whether the specified Area is a stub area or not. The possible values are enabled and disabled. This is a configured value.
Import Summary LSAs	Shows whether to import summary LSAs (enabled).
OSPF Stub Metric Value	The metric value of the stub area. This field displays only if the area is configured as a stub area.

The following OSPF NSSA specific information displays only if the area is configured as an NSSA.

Term	Definition
Import Summary LSAs	Shows whether to import summary LSAs into the NSSA.
Redistribute into NSSA	Shows whether to redistribute information into the NSSA.
Default Information Originate	Shows whether to advertise a default route into the NSSA.
Default Metric	The metric value for the default route advertised into the NSSA.
Default Metric Type	The metric type for the default route advertised into the NSSA.

Term	Definition
Translator Role	The NSSA translator role of the ABR, which is always or candidate.
Translator Stability Interval	The amount of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.
Translator State	Shows whether the ABR translator state is disabled, always, or elected.

show ipv6 ospf asbr

M4350

This command displays the internal OSPFv3 routes to reach Autonomous System Boundary Routers (ASBR).

Format	<code>show ipv6 ospf asbr</code>
Modes	Privileged EXEC User EXEC

Term	Definition
Type	The type of the route to the destination. It can be either: • intra. Intra-area route • inter. Inter-area route
Router ID	Router ID of the destination.
Cost	Cost of using this route.
Area ID	The area ID of the area from which this route is learned.
Next Hop	Next hop toward the destination.
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

show ipv6 ospf database

M4350

This command displays information about the link state database when OSPFv3 is enabled. If you do not enter any parameters, the command displays the LSA headers for all areas. Use the optional *area-id* parameter to display database information about a specific area.

Use the other optional parameters to specify the type of link state advertisements to display:

- Use **external** to display the external LSAs.
- Use **inter-area** to display the inter-area LSAs.
- Use **link** to display the link LSAs.
- Use **network** to display the network LSAs.
- Use **nssa-external** to display NSSA external LSAs.

- Use **prefix** to display intra-area Prefix LSAs.
- Use **router** to display router LSAs.
- Use **unknown area**, **unknown as**, or **link** to display unknown area, AS or link-scope LSAs, respectively.
- As an option, use *lsid* to specify the link state ID (LSID).
- Use **adv-router** to show the LSAs that are restricted by the advertising router. AS an option, use *rtrid* to specify the router ID.
- Use **self-originate** to display the LSAs in that are self originated.

Information is displayed only if OSPF is enabled.

Format	<code>show ipv6 ospf [area-id] database [{external inter-area {prefix router} link network nssa-external prefix router unknown {area as link}}] [lsid] [{adv-router [rtrid] self-originate}]</code>
Modes	Privileged EXEC User EXEC

For each link-type and area, the following information is displayed.

Term	Definition
Link Id	A number that uniquely identifies an LSA that a router originates from all other self originated LSAs of the same LS type.
Adv Router	The Advertising Router. Is a 32-bit dotted decimal number representing the LSDB interface.
Age	A number representing the age of the link state advertisement in seconds.
Sequence	A number that represents which LSA is more recent.
Checksum	The total number LSA checksum.
Prefix	The IPv6 prefix.
Interface	The interface for the link.
Rtr Count	The number of routers attached to the network.

`show ipv6 ospf database database-summary`

M4350

Use this command to display the number of each type of LSA in the database and the total number of LSAs in the database.

Format	<code>show ipv6 ospf database database-summary</code>
Modes	Privileged EXEC User EXEC

Term	Definition
Router	Total number of router LSAs in the OSPFv3 link state database.
Network	Total number of network LSAs in the OSPFv3 link state database.
Inter-area Prefix	Total number of inter-area prefix LSAs in the OSPFv3 link state database.
Inter-area Router	Total number of inter-area router LSAs in the OSPFv3 link state database.
Type-7 Ext	Total number of NSSA external LSAs in the OSPFv3 link state database.
Link	Total number of link LSAs in the OSPFv3 link state database.
Intra-area Prefix	Total number of intra-area prefix LSAs in the OSPFv3 link state database.
Link Unknown	Total number of link-source unknown LSAs in the OSPFv3 link state database.
Area Unknown	Total number of area unknown LSAs in the OSPFv3 link state database.
AS Unknown	Total number of as unknown LSAs in the OSPFv3 link state database.
Type-5 Ext	Total number of AS external LSAs in the OSPFv3 link state database.
Self-Originated Type-5	Total number of self originated AS external LSAs in the OSPFv3 link state database.
Total	Total number of router LSAs in the OSPFv3 link state database.

show ipv6 ospf interface

M4350

This command displays the information for the physical interface or virtual interface tables.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* can be a number from 1–4093.

You can use the **loopback** keyword and *loopback-id* argument to specify a loopback interface.

Format	<code>show ipv6 ospf interface {unit/slot/port vlan vlan-id loopback loopback-id}</code>
Modes	Privileged EXEC User EXEC

Term	Definition
IP Address	The IPv6 address of the interface.
ifIndex	The interface index number associated with the interface.
OSPF Admin Mode	Shows whether the admin mode is enabled or disabled.
OSPF Area ID	The area ID associated with this interface.

Term	Definition
Router Priority	The router priority. The router priority determines which router is the designated router.
Retransmit Interval	The frequency, in seconds, at which the interface sends LSA.
Hello Interval	The frequency, in seconds, at which the interface sends Hello packets.
Dead Interval	The amount of time, in seconds, the interface waits before assuming a neighbor is down.
LSA Ack Interval	The amount of time, in seconds, the interface waits before sending an LSA acknowledgement after receiving an LSA.
Interface Transmit Delay	The number of seconds the interface adds to the age of LSA packets before transmission.
Authentication Type	The type of authentication the interface performs on LSAs it receives.
Metric Cost	The priority of the path. Low costs have a higher priority than high costs.
Prefix-suppression	Displays whether prefix-suppression is enabled, disabled, or unconfigured on the specified interface.
Passive Status	Shows whether the interface is passive or not.
OSPF MTU-ignore	Shows whether to ignore MTU mismatches in database descriptor packets sent from neighboring routers.
Link LSA Suppression	The configured state of Link LSA Suppression for the interface.

The following information only displays if OSPF is initialized on the interface.

Term	Definition
OSPF Interface Type	Broadcast LANs, such as Ethernet and IEEE 802.5, take the value broadcast. The OSPF Interface Type is broadcast.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.
Designated Router	The router ID representing the designated router.
Backup Designated Router	The router ID representing the backup designated router.
Number of Link Events	The number of link events.
Metric Cost	The cost of the OSPF interface.

show ipv6 ospf interface brief

M4350

This command displays brief information for the physical interface or virtual interface tables.

Format	<code>show ipv6 ospf interface brief</code>
Modes	Privileged EXEC User EXEC

Term	Definition
Interface	<i>unit/slot/port</i>
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	The OSPF Area ID for the specified interface.
Router Priority	The router priority. The router priority determines which router is the designated router.
Metric Cost	The priority of the path. Low costs have a higher priority than high costs.
Hello Interval	The frequency, in seconds, at which the interface sends Hello packets.
Dead Interval	The amount of time, in seconds, the interface waits before assuming a neighbor is down.
Retransmit Interval	The frequency, in seconds, at which the interface sends LSA.
Retransmit Delay Interval	The number of seconds the interface adds to the age of LSA packets before transmission.
LSA Ack Interval	The amount of time, in seconds, the interface waits before sending an LSA acknowledgement after receiving an LSA.

show ipv6 ospf interface stats

M4350

This command displays the statistics for a specific interface or VLAN. The command displays information only if OSPF is enabled.

Format `show ipv6 ospf interface stats {unit/slot/port | vlan vlan-id}`

Modes Privileged EXEC
User EXEC

Term	Definition
OSPFv3 Area ID	The area id of this OSPF interface.
IP Address	The IP address associated with this OSPF interface.
OSPFv3 Interface Events	The number of times the specified OSPF interface has changed its state, or an error has 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 has changed state, or an error has occurred.
Packets Received	The number of OSPFv3 packets received on the interface.
Packets Transmitted	The number of OSPFv3 packets sent on the interface.
LSAs Sent	The total number of LSAs flooded on the interface.
LSA Acks Received	The total number of LSA acknowledged from this interface.
LSA Acks Sent	The total number of LSAs acknowledged to this interface.

Term	Definition
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.
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.
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.
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. NOTE: Does not apply to Hellos.
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 has been reached for the number of neighbors on an interface or on the system as a whole.

The table in [trapflags \(Router OSPF Config\)](#) on page 1034 lists the number of OSPF packets of each type sent and received on the interface.

show ipv6 ospf lsa-group

M4350

This command displays the number of self-originated LSAs within each LSA group.

Format	show ipv6 ospf lsa-group
Modes	Privileged EXEC User EXEC

Term	Definition
Total self-originated LSAs	The number of LSAs the router is currently originating.
Average LSAs per group	The number of self-originated LSAs divided by the number of LSA groups. The number of LSA groups is the refresh interval (1800 seconds) divided by the pacing interval (configured with the timers pacing lsa-group command) plus two.

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Pacing group limit	The maximum number of self-originated LSAs in one LSA group. If the number of LSAs in a group exceeds this limit, OSPF redistributes LSAs throughout the refresh interval to achieve better balance.
Groups	For each LSA pacing group, the output shows the range of LSA ages in the group and the number of LSAs in the group.

Command example:

```
(R1) #show ipv6 ospf lsa-group
```

```
Total self-originated LSAs:  3019
```

```
Average LSAs per group:  100
```

```
Pacing group limit:  400
```

```
Number of self-originated LSAs within each LSA group...
```

Group	Start Age	Group	End Age	Count
	0		59	96
	60		119	88
	120		179	102
	180		239	95
	240		299	95
	300		359	92
	360		419	48
	420		479	58
	480		539	103
	540		599	99
	600		659	119
	660		719	110
	720		779	106
	780		839	122
	840		899	110
	900		959	99
	960		1019	135
	1020		1079	101
	1080		1139	94
	1140		1199	115
	1200		1259	110
	1260		1319	111
	1320		1379	111
	1380		1439	99
	1440		1499	102
	1500		1559	96
	1560		1619	106
	1620		1679	111

1680	1739	106
1740	1799	80
1800	1859	0
1860	1919	0

show ipv6 ospf max-metric

M4350

This command displays the configured maximum metrics for stub-router mode.

Format	show ipv6 ospf max-metric
Modes	Privileged EXEC User EXEC

Command example:

```
(config)#show ipv6 ospf max-metric
OSPFv3 Router with ID (3.3.3.3)
Start time: 00:00:00, Time elapsed: 00:01:05
Originating router-LSAs with maximum metric
    Condition: on startup for 1000 seconds, State: inactive
    Advertise external-LSAs with metric 16711680
```

show ipv6 ospf neighbor

M4350

This command displays information about OSPF neighbors. If you do not specify a neighbor IP address, the output displays summary information in a table. If you specify an interface, only the information for that interface displays.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* can be a number from 1–4093.

The *ip-address* is the IP address of the neighbor, and when you specify this, detailed information about the neighbor displays. The information displays only if OSPF is enabled and the interface has a neighbor.

Format	show ipv6 ospf neighbor [interface {unit/slot/port vlan vlan-id] [ip-address]
Modes	Privileged EXEC User EXEC

If you do not specify an IP address, a table with the following columns displays for all neighbors or the neighbor associated with the interface that you specify.

Term	Definition
Router ID	The 4-digit dotted-decimal number of the neighbor 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.
Intf ID	The interface ID of the neighbor.
Interface	The interface of the local router in <i>unit/slot/port</i> format.
State	The state of the neighboring routers. Possible values are: • Down. The initial state of the neighbor conversation. No recent information was received from the neighbor. • Attempt. No recent information was received from the neighbor but an attempt was made to contact the neighbor. • Init. An Hello packet from the neighbor was detected, but bidirectional communication is not yet established. • 2 way. Communication between the two routers is bidirectional. • Exchange start. The two neighboring routers attempt to establish the primary router and the initial DD sequence number. • Exchange. The router is sending Database Description packets to the neighbor. • Full. The neighboring routers are fully adjacent and appear in router-LSAs and network-LSAs.
Dead Time	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.
Restart Helper Status	Indicates the status of this router as a helper during a graceful restart of the router specified in the command line: • Helping. The router is acting as a helpful neighbor to the specified router. • Not Helping. The router is not a helpful neighbor at this time.
Restart Reason	When this router is in helpful neighbor mode, this indicates the reason for the restart as provided by the restarting router.
Remaining Grace Time	The number of seconds remaining the in current graceful restart interval. This is displayed only when this router is currently acting as a helpful neighbor for the router specified in the command.
Restart Helper Exit Reason	Indicates the reason that the specified router last exited a graceful restart. • None. Graceful restart has not been attempted • In Progress. Restart is in progress • Completed. The previous graceful restart completed successfully • Timed Out. The previous graceful restart timed out • Topology Changed. The previous graceful restart terminated prematurely because of a topology change

If you specify an IP address for the neighbor router, the following fields display.

Term	Definition
Interface	The interface of the local router in <i>unit/slot/port</i> format.
Area ID	The area ID associated with the interface.
Options	An integer value that indicates the optional OSPF capabilities supported by the neighbor. These are listed in its Hello packets. This enables received Hello Packets to be rejected (that is, neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.
Router Priority	The router priority for the specified interface.
Dead Timer Due	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.
State	The state of the neighboring routers.
Events	Number of times this neighbor relationship has changed state, or an error has occurred.
Retransmission Queue Length	An integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.

show ipv6 ospf range

M4350

This command displays the set of OSPFv3 area ranges configured for a specified area.

Format	<code>show ipv6 ospf range area-id</code>
Modes	Privileged EXEC

Term	Definition
Area ID	The area whose prefixes are summarized.
IPv6 Prefix/Prefix Length	The summary prefix and prefix length.
Type	S (Summary Link) or E (External Link)
Action	Enabled or Disabled
Cost	Metric to be advertised when the range is active.

show ipv6 ospf statistics

M4350

This command displays information about the 15 most recent Shortest Path First (SPF) calculations. SPF is the OSPF routing table calculation.

Format `show ipv6 ospf statistics`

Modes Privileged EXEC
User EXEC

The command displays the following information with the most recent statistics displayed at the end of the table.

Term	Definition
Delta T	The time since the routing table was computed. The time is in the format hours, minutes, and seconds (hh:mm:ss).
Intra	The time taken to compute intra-area routes, in milliseconds.
Summ	The time taken to compute inter-area routes, in milliseconds.
Ext	The time taken to compute external routes, in milliseconds.
SPF Total	The total time taken to compute routes, in milliseconds. The total may exceed the sum of Intra, Summ, and Ext times.
RIB Update	The time from the completion of the routing table calculation until all changes have been made in the common routing table [the Routing Information Base (RIB)], in milliseconds
Reason	The event or events that triggered the SPF. The reason codes are as follows: • R. New router LSA • N. New network LSA • SN. New network (inter-area prefix) summary LSA • SA. New ASBR (inter-area router) summary LSA • X. New external LSA • IP. New intra-area prefix LSA • L. New Link LSA

Command example:

```
(NETGEAR Switch) #show ipv6 ospf statistics
```

```
Area 0.0.0.0: SPF algorithm executed 10 times
```

Delta T	Intra	Summ	Ext	SPF Total	RIB Update	Reason
23:32:46	0	0	0	0	0	R, IP
23:32:09	0	0	0	0	0	R, N, IP
23:32:04	0	0	0	0	0	R
23:31:44	0	0	0	0	0	R, N, IP

Fully Managed Switches M4250 and M4350 Series

23:31:39	0	0	0	0	1	R
23:29:57	0	3	7	10	131	R
23:29:52	0	14	29	43	568	SN
04:07:23	0	9	23	33	117	SN
04:07:23	0	9	23	33	117	SN
04:07:18	0	0	0	1	485	SN
04:07:14	0	1	0	1	3	X

show ipv6 ospf stub table

M4350

This command displays the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

Format	show ipv6 ospf stub table
Modes	Privileged EXEC User EXEC
Term	Definition
Area ID	A 32-bit identifier for the created stub area.
Type of Service	Type of service associated with the stub metric. For this release, Normal TOS is the only supported type.
Metric Val	The metric value is applied based on the TOS. It defaults to the least metric of the type of service among the interfaces to other areas. The OSPF cost for a route is a function of the metric value.
Import Summary LSA	Controls the import of summary LSAs into stub areas.

show ipv6 ospf virtual-link

M4350

This command displays the OSPF Virtual Interface information for a specific area and neighbor. The *area-id* parameter identifies the area and the *neighbor* parameter identifies the neighbor's Router ID.

Format	show ipv6 ospf virtual-link area-id neighbor
Modes	Privileged EXEC User EXEC
Term	Definition
Area ID	The area id of the requested OSPF area.
Neighbor Router ID	The input neighbor Router ID.

Term	Definition
Hello Interval	The configured hello interval for the OSPF virtual interface.
Dead Interval	The configured dead interval for the OSPF virtual interface.
Interface Transmit Delay	The configured transmit delay for the OSPF virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.
Authentication Type	The type of authentication the interface performs on LSAs it receives.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPF interface.
Neighbor State	The neighbor state.

show ipv6 ospf virtual-link brief

M4350

This command displays the OSPFV3 Virtual Interface information for all areas in the system.

Format `show ipv6 ospf virtual-link brief`

Modes Privileged EXEC
User EXEC

Term	Definition
Area ID	The area id of the requested OSPFV3 area.
Neighbor	The neighbor interface of the OSPFV3 virtual interface.
Hello Interval	The configured hello interval for the OSPFV3 virtual interface.
Dead Interval	The configured dead interval for the OSPFV3 virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPFV3 virtual interface.
Transmit Delay	The configured transmit delay for the OSPFV3 virtual interface.

DHCPv6 Commands

This section describes the commands you use to configure the DHCPv6 server on the system and to view DHCPv6 information.

service dhcpv6

M4250

M4350

This command enables DHCPv6 configuration on the router.

Default	enabled
Format	service dhcpv6
Mode	Global Config

no service dhcpv6

This command disables DHCPv6 configuration on router.

Format	no service dhcpv6
Mode	Global Config

ipv6 dhcp client pd

M4250

M4350

Use this command to enable the Dynamic Host Configuration Protocol (DHCP) for IPv6 client process (if the process is not currently running) and to enable requests for prefix delegation through a specified interface. When prefix delegation is enabled and a prefix is successfully acquired, the prefix is stored in the IPv6 general prefix pool with an internal name defined by the automatic argument.

Note: The Prefix Delegation client is supported on only one IP interface.

The optional **rapid-commit** keyword enables the use of a two-message exchange method for prefix delegation and other configuration. If enabled, the client includes the rapid commit option in a solicit message.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. If one of these functions is already enabled and a user tries to configure a different function on the same interface, a message is displayed.

Default	Prefix delegation is disabled on an interface.

Format	ipv6 dhcp client pd [rapid-commit]

Mode	Interface Config

Command example: The following examples enable prefix delegation on interface 1/0/1:

```
(NETGEAR Switch) #configure
(NETGEAR Switch) (Config)#interface 1/0/1
(NETGEAR Switch) (Interface 1/0/1)# ipv6 dhcp client pd
```

```
(NETGEAR Switch) #configure
(NETGEAR Switch) (Config)#interface 1/0/1
(NETGEAR Switch) (Interface 1/0/1)# ipv6 dhcp client pd rapid-commit
```

no ipv6 dhcp client pd

This command disables requests for prefix delegation.

Format	no ipv6 dhcp client pd

Mode	Interface Config

ipv6 dhcp conflict logging

M4250

M4350

This command enables the logging of the bindings reported to be conflicting by DHCPv6 clients using DECLINE messages.

Default	Enabled

Format	ipv6 dhcp conflict logging

Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config)#ipv6 dhcp conflict logging
```

no ipv6 dhcp conflict logging

This command disables the logging of the bindings reported to be conflicting by DHCPv6 clients.

Format	no ipv6 dhcp conflict logging

Mode	Global Config

ipv6 dhcp server

M4250

M4350

Use this command to configure DHCPv6 server functionality on an interface or range of interfaces. The *pool-name* is the DHCPv6 pool containing stateless and/or prefix delegation parameters, **automatic** enables the server to automatically determine which pool to use when allocating addresses for a client, **rapid-commit** is an option that allows for an abbreviated exchange between the client and server, and *pref-value* is a value used by clients to determine preference between multiple DHCPv6 servers. For a particular interface, DHCPv6 server and DHCPv6 relay functions are mutually exclusive.

Format	ipv6 dhcp server { <i>pool-name</i> automatic} [rapid-commit] [preference <i>pref-value</i>]

Mode	Interface Config

no ipv6 dhcp server

This command disables DHCPv6 server functionality on an interface.

Format	no ipv6 dhcp server

Mode	Interface Config

ipv6 dhcp relay

M4250

M4350

Use this command to configure an interface for DHCPv6 relay functionality on an interface or range of interfaces.

- Use the **destination** keyword to set the relay server IPv6 address.
- The *relay-address* parameter is an IPv6 address of a DHCPv6 relay server.
- Use the **interface** keyword to set the relay server interface. The *relay-interface* parameter is an interface (*slot/port* for an M4250 series switch or *unit/slot/port* for an M4350 series switch) or VLAN that can reach a relay server.

- The optional **remote-id** is the Relay Agent Information Option remote ID suboption to be added to relayed messages. This can either be the special keyword **duid-uuid**, which causes the remote ID to be derived from the DHCPv6 server DUID and the relay interface number, or it can be specified as a *user-defined string*.

Note: If *relay-address* is an IPv6 global address, then *relay-interface* is not required. If *relay-address* is a link-local or multicast address, then *relay-interface* is required. Finally, if you do not specify a value for *relay-address*, then you must specify a value for *relay-interface* and the DHCPV6-ALL-AGENTS multicast address (for example, FF02::1:2) is used to relay DHCPv6 messages to the relay server.

Format	<code>ipv6 dhcp relay {destination <i>relay-address</i> interface {<i>unit/slot/port</i> <i>vlan vlan-id</i>} interface {<i>unit/slot/port</i> <i>vlan vlan-id</i>} remote-id {<i>duid-uuid</i> <i>user-defined-string</i>}}</code>

Mode	Interface Config

no ipv6 dhcp relay

This command removes the specified DHCPv6 relay.

Format	<code>no ipv6 dhcp relay [destination <i>relay-address</i> interface {<i>unit/slot/port</i> <i>vlan vlan-id</i>} interface {<i>unit/slot/port</i> <i>vlan vlan-id</i>} remote-id {<i>duid-uuid</i> <i>user-defined-string</i>}]</code>

Mode	Interface Config

ipv6 dhcp pool

M4250

M4350

Use this command from Global Config mode to enter IPv6 DHCP Pool Config mode. Use the **exit** command to return to Global Config mode. To return to the User EXEC mode, enter **Ctrl+Z**. The *pool-name* must be less than 31 alpha-numeric characters. DHCPv6 pools are used to specify information for DHCPv6 server to distribute to DHCPv6 clients. These pools are shared between multiple interfaces over which DHCPv6 server capabilities are configured.

Once the DHCP for IPv6 configuration information pool has been created, use the **ipv6 dhcp server** command to associate the pool with a server on an interface. If you do not configure an information pool, use the **ipv6 dhcp server** interface configuration command to enable the DHCPv6 server function on an interface.

When you associate a DHCPv6 pool with an interface, only that pool services requests on the associated interface. The pool also services other interfaces. If you do not associate a

DHCPv6 pool with an interface, it can service requests on any interface. Not using any IPv6 address prefix means that the pool returns only configured options.

Format	<code>ipv6 dhcp pool <i>pool-name</i></code>

Mode	Global Config

`no ipv6 dhcp pool`

This command removes the specified DHCPv6 pool.

Format	<code>no ipv6 dhcp pool <i>pool-name</i></code>

Mode	Global Config

address prefix (IPv6 DHCP Pool Config)

M4250

M4350

Use this command to sets an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons.

If **lifetime** values are not configured, the default lifetime values for *valid-lifetime* and *preferred-lifetime* are considered to be infinite.

Format	<code>address prefix <i>prefix/prefixlength</i> [lifetime {<i>valid-lifetime</i> <i>preferred-lifetime</i> infinite}]</code>

Mode	IPv6 DHCP Pool Config

Term	Definition
lifetime	(Optional) Sets a length of time for the hosts to remember router advertisements. If configured, both valid and preferred lifetimes must be configured.
<i>valid-lifetime</i>	The amount of time, in seconds, the prefix remains valid for the requesting router to use. The range is from 60 through 4294967294. The <i>preferred-lifetime</i> value cannot exceed the <i>valid-lifetime</i> value.
<i>preferred-lifetime</i>	The amount of time, in seconds, that the prefix remains preferred for the requesting router to use. The range is from 60 through 4294967294. The <i>preferred-lifetime</i> value cannot exceed the <i>valid-lifetime</i> value.
infinite	An unlimited lifetime.

Command example:

The following example configures an IPv6 address prefix for the IPv6 configuration pool pool1:

```
(NETGEAR Switch) #configure
(NETGEAR Switch) (Config)# ipv6 dhcp pool pool1
```

```
(NETGEAR Switch) (Config-dhcp6s-pool)# address prefix 2001::/64
(NETGEAR Switch) (Config-dhcp6s-pool)# exit
```

no address prefix (IPv6 DHCP Pool Config)

This command removes the specified address prefix.

Format	<code>no address prefix <i>prefix/prefixlength</i></code>
Mode	IPv6 DHCP Pool Config

domain-name (IPv6 DHCP Pool Config)

M4250

M4350

This command sets the DNS domain name which is provided to DHCPv6 client by DHCPv6 server. DNS domain name is configured for stateless server support. Domain name consist of no more than 31 alpha-numeric characters. DHCPv6 pool can have multiple number of domain names with maximum of 8.

Format	<code>domain-name <i>domain-name</i></code>
Mode	IPv6 DHCP Pool Config

no domain-name (IPv6 DHCP Pool Config)

This command removes DHCPv6 domain name from dhcpv6 pool.

Format	<code>no domain-name <i>domain-name</i></code>
Mode	IPv6 DHCP Pool Config

dns-server (IPv6 DHCP Pool Config)

M4250

M4350

This command sets the IPv6 DNS server address, which is provided to DHCPv6 clients by the DHCPv6 server. The DNS server address is configured for stateless server support. The DHCPv6 pool can contains a maximum of eight domain names.

Format	<code>dns-server <i>ipv6-address</i></code>
Mode	IPv6 DHCP Pool Config

no dns-server (IPv6 DHCP Pool Config)

This command removes a DHCPv6 server address from a DHCPv6 server.

Format	<code>no dns-server ipv6-address</code>

Mode	IPv6 DHCP Pool Config

prefix-delegation (IPv6 DHCP Pool Config)

M4250

M4350

Multiple IPv6 prefixes can be defined within a pool for distributing to specific DHCPv6 prefix delegation clients.

- *prefix* is the delegated IPv6 prefix and *prefixlength* is the associated prefix length.
- *duid* is the client's unique DUID value, for example, 00:01:00:09:f8:79:4e:00:04:76:73:43:76.
- *hostname* is 31 characters textual client's name which is useful for logging or tracing only.
- valid lifetime is the valid lifetime for the delegated prefix in *seconds*, in a range from 0–4294967295 seconds, or infinite.
- preferred lifetime is the preferred lifetime for the delegated prefix in *seconds*, in a range from 0–4294967295 seconds, or infinite.

Default	valid-lifetime <i>seconds</i> : 2592000 preferred-lifetime <i>seconds</i> : 604800

Format	<code>prefix-delegation prefix/prefixlength duid [name hostname] [valid-lifetime {seconds infinite}] [preferred-lifetime {seconds infinite}]</code>

Mode	IPv6 DHCP Pool Config

no prefix-delegation (IPv6 DHCP Pool Config)

This command deletes a specific prefix-delegation client.

Format	<code>no prefix-delegation prefix/prefix-delegation duid</code>

Mode	IPv6 DHCP Pool Config

show ipv6 dhcp

M4250

M4350

This command displays the DHCPv6 server name and status.

Format	show ipv6 dhcp
Mode	Privileged EXEC
Term	Definition
DHCPv6 is Enabled (Disabled)	The status of the DHCPv6 server.
Server DUID	If configured, shows the DHCPv6 unique identifier.

show ipv6 dhcp statistics

M4250

M4350

This command displays the IPv6 DHCP statistics for all interfaces.

Format	show ipv6 dhcp statistics
Mode	Privileged EXEC
Term	Definition
DHCPv6 Solicit Packets Received	Number of solicit received statistics.
DHCPv6 Request Packets Received	Number of request received statistics.
DHCPv6 Confirm Packets Received	Number of confirm received statistics.
DHCPv6 Renew Packets Received	Number of renew received statistics.
DHCPv6 Rebind Packets Received	Number of rebind received statistics.
DHCPv6 Release Packets Received	Number of release received statistics.
DHCPv6 Decline Packets Received	Number of decline received statistics.
DHCPv6 Inform Packets Received	Number of inform received statistics.
DHCPv6 Relay-forward Packets Received	Number of relay forward received statistics.
DHCPv6 Relay-reply Packets Received	Number of relay-reply received statistics.
DHCPv6 Malformed Packets Received	Number of malformed packets statistics.
Received DHCPv6 Packets Discarded	Number of DHCP discarded statistics.

Term	Definition
Total DHCPv6 Packets Received	Total number of DHCPv6 received statistics
DHCPv6 Advertisement Packets Transmitted	Number of advertise sent statistics.
DHCPv6 Reply Packets Transmitted	Number of reply sent statistics.
DHCPv6 Reconfig Packets Transmitted	Number of reconfigure sent statistics.
DHCPv6 Relay-reply Packets Transmitted	Number of relay-reply sent statistics.
DHCPv6 Relay-forward Packets Transmitted	Number of relay-forward sent statistics.
Total DHCPv6 Packets Transmitted	Total number of DHCPv6 sent statistics.

show ipv6 dhcp interface

M4250

M4350

This command displays DHCPv6 information for all relevant interfaces or the specified interface.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* can be a number from 1–4093.

If you specify an interface, you can use the optional **statistics** keyword to view statistics for the specified interface.

Format	<code>show ipv6 dhcp interface {unit/slot/port vlan vlan-id} [statistics]</code>
Mode	Privileged EXEC

Term	Definition
IPv6 Interface	The interface name.
Mode	Shows whether the interface is a IPv6 DHCP relay or server.

If the interface mode is server, the following information displays.

Term	Definition
Pool Name	The pool name specifying information for DHCPv6 server distribution to DHCPv6 clients.

Term	Definition
Server Preference	The preference of the server.
Option Flags	Shows whether rapid commit is enabled.

If the interface mode is relay, the following information displays.

Term	Definition
Relay Address	The IPv6 address of the relay server.
Relay Interface Number	The relay server interface.
Relay Remote ID	If configured, shows the name of the relay remote.
Option Flags	Shows whether rapid commit is configured.

If you use the statistics parameter, the command displays the IPv6 DHCP statistics for the specified interface. See [show ipv6 dhcp statistics on page 1252](#) for information about the output.

show ipv6 dhcp binding

M4250

M4350

This command displays configured DHCP pool.

Format	show ipv6 dhcp binding [ipv6-address]
Mode	Privileged EXEC

Term	Definition
DHCP Client Address	Address of DHCP Client.
DUID	String that represents the Client DUID.
IAID	Identity Association ID.
Prefix/Prefix Length	IPv6 address and mask length for delegated prefix.
Prefix Type	IPV6 Prefix type (IAPD, IANA, or IATA).
Client Address	Address of DHCP Client.
Client Interface	IPv6 Address of DHCP Client.
Expiration	Address of DNS server address.

Term	Definition
Valid Lifetime	Valid lifetime in seconds for delegated prefix.
Preferred Lifetime	Preferred lifetime in seconds for delegated prefix.

show ipv6 dhcp pool

M4250

M4350

This command displays configured or automatic DHCP pools.

Format	<code>show ipv6 dhcp pool {pool-name automatic}</code>
Mode	Privileged EXEC

Term	Definition
DHCP Pool Name	Unique pool name configuration.
Client DUID	Client's DHCP unique identifier. DUID is generated using the combination of the local system burned-in MAC address and a timestamp value.
Host	Name of the client.
Prefix/Prefix Length	IPv6 address and mask length for delegated prefix.
Preferred Lifetime	Preferred lifetime in seconds for delegated prefix.
Valid Lifetime	Valid lifetime in seconds for delegated prefix.
DNS Server Address	Address of DNS server address.
Domain Name	DNS domain name.

show ipv6 dhcp conflict

M4250

M4350

This command displays any conflict bindings on the DHCPv6 server that might be created when leased bindings are declined by DHCPv6 clients. You can also limit the output to a specific IPv6 address.

Format	<code>show ipv6 dhcp conflict [ipv6-address]</code>
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch)#show ipv6 dhcp conflict
```

```
Pool Name..... STATEFUL
Prefix..... 2001::/64
Conflict Bindings..... 2001::2
..... 2001::3
```

show serviceport ipv6 dhcp statistics

M4250**M4350**

This command displays the statistics of the DHCPv6 client running on the serviceport management interface.

Format	show serviceport ipv6 dhcp statistics

Mode	Privileged EXEC User EXEC

Field	Description
DHCPv6 Advertisement Packets Received	The number of DHCPv6 Advertisement packets received on the service port interface.
DHCPv6 Reply Packets Received	The number of DHCPv6 Reply packets received on the service port interface.
Received DHCPv6 Advertisement Packets Discarded	The number of DHCPv6 Advertisement packets discarded on the service port interface.
Received DHCPv6 Reply Packets Discarded	The number of DHCPv6 Reply packets discarded on the service port interface.
DHCPv6 Malformed Packets Received	The number of DHCPv6 packets that are received malformed on the service port interface.
Total DHCPv6 Packets Received	The total number of DHCPv6 packets received on the service port interface.
DHCPv6 Solicit Packets Transmitted	The number of DHCPv6 Solicit packets transmitted on the service port interface.
DHCPv6 Request Packets Transmitted	The number of DHCPv6 Request packets transmitted on the service port interface.
DHCPv6 Renew Packets Transmitted	The number of DHCPv6 Renew packets transmitted on the service port interface.
DHCPv6 Rebind Packets Transmitted	The number of DHCPv6 Rebind packets transmitted on the service port interface.

Field	Description
DHCPv6 Release Packets Transmitted	The number of DHCPv6 Release packets transmitted on the service port interface.
Total DHCPv6 Packets Transmitted	The total number of DHCPv6 packets transmitted on the service port interface.

Command example:

```
(Netgear switch) #show serviceport ipv6 dhcp statistics
DHCPv6 Client Statistics
-----

DHCPv6 Advertisement Packets Received..... 0
DHCPv6 Reply Packets Received..... 0
Received DHCPv6 Advertisement Packets Discarded..... 0
Received DHCPv6 Reply Packets Discarded..... 0
DHCPv6 Malformed Packets Received..... 0
Total DHCPv6 Packets Received..... 0

DHCPv6 Solicit Packets Transmitted..... 0
DHCPv6 Request Packets Transmitted..... 0
DHCPv6 Renew Packets Transmitted..... 0
DHCPv6 Rebind Packets Transmitted..... 0
DHCPv6 Release Packets Transmitted..... 0
Total DHCPv6 Packets Transmitted..... 0
```

clear ipv6 dhcp**M4250****M4350**

Use this command to clear DHCPv6 statistics for all interfaces or for a specific interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	<code>clear ipv6 dhcp {statistics interface {unit/slot/port vlan vlan-id} statistics}</code>
Mode	Privileged EXEC

clear ipv6 dhcp binding

M4250**M4350**

This command deletes an automatic address binding from the DHCP server database.

A binding table entry on the DHCP for IPv6 server is automatically:

- Created whenever a prefix is delegated to a client from the configuration pool.
- Updated when the client renews, rebinds, or confirms the prefix delegation.
- Deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired or when you enter the **clear ipv6 dhcp binding** command.

If the **clear ipv6 dhcp binding** command is used with the optional *ipv6-address* argument, only the binding for the specified client is deleted. If the **clear ipv6 dhcp binding** command is used without the *ipv6-address* argument, all automatic client bindings are deleted from the DHCP for IPv6 binding table.

Format	<code>clear ipv6 dhcp binding [ipv6-address]</code>
Mode	Privileged EXEC

clear network ipv6 dhcp statistics

M4250**M4350**

Use this command to clear the DHCPv6 statistics on the network management interface.

Format	<code>clear network ipv6 dhcp statistics</code>
Mode	Privileged EXEC

clear serviceport ipv6 dhcp statistics

M4250**M4350**

Use this command to clear the DHCPv6 client statistics on the service port interface.

Format	<code>clear serviceport ipv6 dhcp statistics</code>
Mode	Privileged EXEC

DHCPv6 Snooping Configuration Commands

This section describes commands you use to configure IPv6 DHCP Snooping.

ipv6 dhcp snooping

M4250

M4350

Use this command to globally enable IPv6 DHCP Snooping.

Default	disabled
Format	ipv6 dhcp snooping
Mode	Global Config

no ipv6 dhcp snooping

Use this command to globally disable IPv6 DHCP Snooping.

Format	no ipv6 dhcp snooping
Mode	Global Config

ipv6 dhcp snooping vlan

M4250

M4350

Use this command to enable DHCP Snooping on a list of comma-separated VLAN ranges.

Default	disabled
Format	ipv6 dhcp snooping vlan <i>vlan-list</i>
Mode	Global Config

no ipv6 dhcp snooping vlan

Use this command to disable DHCP Snooping on VLANs.

Format	no ipv6 dhcp snooping vlan <i>vlan-list</i>
Mode	Global Config

ipv6 dhcp snooping verify mac-address

M4250

M4350

Use this command to enable verification of the source MAC address with the client hardware address in the received DHCP message.

Default	enabled
Format	ipv6 dhcp snooping verify mac-address
Mode	Global Config

no ipv6 dhcp snooping verify mac-address

Use this command to disable verification of the source MAC address with the client hardware address.

Format	no ipv6 dhcp snooping verify mac-address
Mode	Global Config

ipv6 dhcp snooping database

M4250

M4350

Use this command to configure the persistent location of the DHCP Snooping database. This can be local or a remote file.

Default	local
Format	ipv6 dhcp snooping database {local tftp://hostIP/filename}
Mode	Global Config

ip dhcp snooping database write-delay (DHCPv6)

M4250

M4350

Use this command to configure the interval in seconds at which the DHCP Snooping database is persisted. For the *seconds* argument, the interval value is in a range from 15 to 86400 seconds.

Default	300 seconds
Format	ip dhcp snooping database write-delay <i>seconds</i>
Mode	Global Config

no ip dhcp snooping database write-delay

Use this command to set the write delay value to the default value.

Format	no ip dhcp snooping database write-delay

Mode	Global Config

ipv6 dhcp snooping binding

M4250

M4350

Use this command to configure a static DHCP Snooping binding. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Only the expiry **keyword** is optional, for which the *seconds* argument specifies the expiration time for the static entry.

Format	ipv6 dhcp snooping binding { <i>mac-address</i> } {vlan <i>vlan-id</i> } { <i>ipaddress</i> } {interface { <i>unit/slot/port</i> lag <i>lag-intf-num</i> }} [expiry <i>seconds</i>]

Mode	Global Config

no ipv6 dhcp snooping binding

Use this command to remove the DHCP static entry from the DHCP Snooping database.

Format	no ipv6 dhcp snooping binding <i>mac-address</i>

Mode	Global Config

ipv6 dhcp snooping trust

M4250

M4350

Use this command to configure an interface or range of interfaces as trusted.

Default	disabled

Format	ipv6 dhcp snooping trust

Mode	Interface Config

no ipv6 dhcp snooping trust

Use this command to configure the port as untrusted.

Format	no ipv6 dhcp snooping trust
Mode	Interface Config

ipv6 dhcp snooping log-invalid

M4250

M4350

Use this command to control the logging DHCP messages filtration by the DHCP Snooping application. This command can be used to configure a single interface or a range of interfaces.

Default	disabled
Format	ipv6 dhcp snooping log-invalid
Mode	Interface Config

no ipv6 dhcp snooping log-invalid

Use this command to disable the logging DHCP messages filtration by the DHCP Snooping application.

Format	no ipv6 dhcp snooping log-invalid
Mode	Interface Config

ipv6 dhcp snooping limit

M4250

M4350

Use this command to control the rate at which the DHCP Snooping messages come on an interface or range of interfaces.

By default, rate-limiting is disabled. When enabled, the rate can range from 0 to 300 packets per second, which is expressed in the *pps* argument. The burst level range is 1 to 15 seconds, which is expressed in the *seconds* argument. Rate-limiting is configured on a physical port and may be applied to trusted and untrusted ports.

By default, rate-limiting is disabled. You can also use the **none** keyword to disable rate-limiting on incoming DHCP Snooping messages.

Default	disabled (no limit)
Format	<code>ipv6 dhcp snooping limit {rate pps [burst interval seconds] none}</code>
Mode	Interface Config

`no ipv6 dhcp snooping limit`

Use this command to set the rate at which the DHCP Snooping messages enter the switch and the associated burst level to the defaults.

Format	<code>no ipv6 dhcp snooping limit</code>
Mode	Interface Config

`ipv6 verify source`

M4250

M4350

Use this command to configure the IPv6SG source ID attribute to filter the data traffic in the hardware. Source ID is the combination of IP address and MAC address. Normal command allows data traffic filtration based on the IP address. With the **port-security** option, the data traffic is filtered based on the IP and MAC addresses.

This command can be used to configure a single interface or a range of interfaces.

Default	The source ID is the IP address
Format	<code>ipv6 verify source {port-security}</code>
Mode	Interface Config

`no ipv6 verify source`

Use this command to disable the IPv6SG configuration in the hardware. You cannot disable port-security alone if it is configured.

Format	<code>no ipv6 verify source</code>
Mode	Interface Config

ipv6 verify binding

M4250

M4350

Use this command to configure static IPv6 source guard (IPv6SG) entries. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>ipv6 verify binding {mac-address} {vlan vlan-id} {ipaddress} {interface {unit/slot/port lag lag-intf-num}}</code>
Mode	Global Config

no ipv6 verify binding

Use this command to remove the IPv6SG static entry from the IPv6SG database.

Format	<code>no ipv6 verify binding {mac-address} {vlan vlan-id} {ipaddress} {interface {unit/slot/port lag lag-intf-num}}</code>
Mode	Global Config

show ipv6 dhcp snooping

M4250

M4350

Use this command to display the DHCP Snooping global configurations and per port configurations.

Format	<code>show ipv6 dhcp snooping</code>
Mode	Privileged EXEC User EXEC

Term	Definition
Interface	The interface for which data is displayed.
Trusted	If it is enabled, DHCP snooping considers the port as trusted. The factory default is disabled.
Log Invalid Pkts	If it is enabled, DHCP snooping application logs invalid packets on the specified interface.

Command example:

```
(NETGEAR Switch) #show ipv6 dhcp snooping
```

```
DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
11 - 30, 40
```

Interface	Trusted	Log Invalid Pkts
0/1	Yes	No
0/2	No	Yes
0/3	No	Yes
0/4	No	No
0/6	No	No

show ipv6 dhcp snooping binding**M4250****M4350**

Use this command to display the DHCP Snooping binding entries. To restrict the output, use the following options:

- **static**. Restrict the output based on static entries.
- **dynamic**. Restrict the output based on DHCP snooping.
- **interface** *unit/slot/port*. Restrict the output based on a specific interface. To specify an actual interface or port, do the following:
 - For an M4250 series switch, use the argument *slot/port*.
 - For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.
- **vlan** *vlan-id*. Restrict the output based on a VLAN.

Format	<code>show ipv6 dhcp snooping binding [static dynamic] [interface <i>unit/slot/port</i>] [vlan <i>vlan-id</i>]</code>

Mode	Privileged EXEC User EXEC

Term	Definition
MAC Address	Displays the MAC address for the binding that was added. The MAC address is the key to the binding database.
IPv6 Address	Displays the valid IPv6 address for the binding rule.
VLAN	The VLAN for the binding rule.

Term	Definition
Interface	The interface to add a binding into the DHCP snooping interface.
Type	Binding type; statically configured from the CLI or dynamically learned.
Lease (sec)	The remaining lease time for the entry.

Command example:

```
(NETGEAR Switch) #show ipv6 dhcp snooping binding
Total number of bindings: 2
```

MAC Address	IPv6 Address	VLAN	Interface	Type	Lease time (Secs)
00:02:B3:06:60:80	2000::1/64	10	0/1		86400
00:0F:FE:00:13:04	3000::1/64	10	0/1		86400

show ipv6 dhcp snooping database**M4250****M4350**

Use this command to display the DHCP Snooping configuration related to the database persistency.

Format	show ipv6 dhcp snooping database
Mode	Privileged EXEC User EXEC

Term	Definition
Agent URL	Bindings database agent URL.
Write Delay	The maximum write time to write the database into local or remote.

Command example:

```
(NETGEAR Switch) #show ipv6 dhcp snooping database
agent url: /10.131.13.79:/sail.txt
write-delay: 5000
```


show ipv6 dhcp snooping interfaces

M4250**M4350**

Use this command to show the DHCP Snooping status of all interfaces or a specified interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show ipv6 dhcp snooping interfaces [<i>unit/slot/port</i>]

Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show ipv6 dhcp snooping interfaces
```

Interface	Trust State	Rate Limit (pps)	Burst Interval (seconds)
1/0/1	No	151	
1/0/2	No	151	
1/0/3	No	151	

```
(NETGEAR Switch) #show ip dhcp snooping interfaces ethernet 1/0/1
```

Interface	Trust State	Rate Limit (pps)	Burst Interval (seconds)
1/0/1	Yes	151	

show ipv6 dhcp snooping statistics

M4250**M4350**

Use this command to list statistics for IPv6 DHCP Snooping security violations on untrusted ports.

Format	show ipv6 dhcp snooping statistics

Mode	Privileged EXEC User EXEC

Term	Definition
Interface	The IPv6 address of the interface in <i>unit/slot/port</i> format.
MAC Verify Failures	Represents the number of DHCP messages that were filtered on an untrusted interface because of source MAC address and client hardware address mismatch.
Client Ifc Mismatch	Represents the number of DHCP release and Deny messages received on the different ports than learned previously.
DHCP Server Msgs Rec'd	Represents the number of DHCP server messages received on Untrusted ports.

Command example:

```
(NETGEAR Switch) #show ipv6 dhcp snooping statistics
```

Interface	MAC Verify Failures	Client Ifc Mismatch	DHCP Server Msgs Rec'd
-----	-----	-----	-----
1/0/2	0	0	0
1/0/3	0	0	0
1/0/4	0	0	0
1/0/5	0	0	0
1/0/6	0	0	0
1/0/7	0	0	0
1/0/8	0	0	0
1/0/9	0	0	0
1/0/10	0	0	0
1/0/11	0	0	0
1/0/12	0	0	0
1/0/13	0	0	0
1/0/14	0	0	0
1/0/15	0	0	0
1/0/16	0	0	0
1/0/17	0	0	0
1/0/18	0	0	0
1/0/19	0	0	0
1/0/20	0	0	0

clear ipv6 dhcp snooping binding

M4250

M4350

Use this command to clear all DHCPv6 Snooping bindings on all interfaces or on a specific interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.

- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>clear ipv6 dhcp snooping binding [interface <i>unit/slot/port</i>]</code>

Mode	Privileged EXEC User EXEC

clear ipv6 dhcp snooping statistics

M4250

M4350

Use this command to clear all DHCPv6 Snooping statistics.

Format	<code>clear ipv6 dhcp snooping statistics</code>

Mode	Privileged EXEC User EXEC

show ipv6 verify

M4250

M4350

Use this command to display the IPv6 configuration on a specified interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show ipv6 verify interface <i>unit/slot/port</i></code>

Mode	Privileged EXEC User EXEC

Term	Definition
Interface	Interface address.
Filter Type	Is one of two values: - ip-v6mac: User has configured MAC address filtering on this interface. - ipv6: Only IPv6 address filtering on this interface.
IPv6 Address	IPv6 address of the interface
MAC Address	If MAC address filtering is not configured on the interface, the MAC Address field is empty. If port security is disabled on the interface, then the MAC Address field displays "permit-all."
VLAN	The VLAN for the binding rule.

Command example:

```
(NETGEAR Switch) #show ipv6 verify 0/1
```

Interface	Filter Type	IP Address	MAC Address	Vlan
-----	-----	-----	-----	-----
0/1	ipv6-mac	2000::1/64	00:02:B3:06:60:80	10
0/1	ipv6-mac	3000::1/64	00:0F:FE:00:13:04	10

show ipv6 verify source

M4250

M4350

Use this command to display the IPv6SG configurations for all ports. To limit the output to an interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.

For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show ipv6 verify source [interface <i>unit/slot/port</i>]

Mode	Privileged EXEC User EXEC

Term	Definition
Interface	Interface address in <i>unit/slot/port</i> format.
Filter Type	Is one of two values: • ip-v6mac: User has configured MAC address filtering on this interface. • ipv6: Only IPv6 address filtering on this interface.
IPv6 Address	IPv6 address of the interface
MAC Address	If MAC address filtering is not configured on the interface, the MAC Address field is empty. If port security is disabled on the interface, then the MAC Address field displays permit-all.
VLAN	The VLAN for the binding rule.

Command example:

```
(NETGEAR Switch) #show ipv6 verify source
```

Interface	Filter Type	IP Address	MAC Address	Vlan
-----	-----	-----	-----	-----
0/1	ipv6-mac	2000::1/64	00:02:B3:06:60:80	10
0/1	ipv6-mac	3000::1/64	00:0F:FE:00:13:04	10

show ipv6 source binding

M4250**M4350**

Use this command to display the IPv6SG bindings. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>show ipv6 source binding [dhcp-snooping static] [interface <i>unit/slot/port</i> <i>vlan vlan-id</i>]</code>
Mode	Privileged EXEC User EXEC
Term	Definition
MAC Address	The MAC address for the entry that is added.
IP Address	The IP address of the entry that is added.
Type	Entry type; statically configured from CLI or dynamically learned from DHCP Snooping.
VLAN	VLAN for the entry.
Interface	IP address of the interface in <i>unit/slot/port</i> format.

Command example:

```
(NETGEAR Switch) #show ipv6 source binding
```

MAC Address	IP Address	Type	Vlan	Interface
-----	-----	-----	-----	-----
00:00:00:00:00:08	2000::1	dhcp-snooping	2	1/0/1
00:00:00:00:00:09	3000::1	dhcp-snooping	3	1/0/1
00:00:00:00:00:0A	4000::1	dhcp-snooping	4	1/0/1

11

Quality of Service Commands

This chapter describes the Quality of Service (QoS) commands.

The chapter contains the following sections:

- [Class of Service Commands](#)
- [Differentiated Services Commands](#)
- [DiffServ Class Commands](#)
- [DiffServ Policy Commands](#)
- [DiffServ Service Commands](#)
- [DiffServ Show Commands](#)
- [MAC Access Control List Commands](#)
- [IP Access Control List Commands](#)
- [IPv6 Access Control List Commands](#)
- [Time Range Commands for Time-Based ACLs](#)
- [Auto-Voice over IP Commands](#)
- [iSCSI Optimization Commands](#)

The commands in this chapter are in one of two functional groups:

- **Show commands.** Display switch settings, statistics, and other information.
- **Configuration commands.** Configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.

Class of Service Commands

This section describes the commands you use to configure and view Class of Service (CoS) settings for the switch. The commands in this section allow you to control the priority and transmission rate of traffic.

Note: Commands you issue in the Interface Config mode only affect a single interface. Commands you issue in the Global Config mode affect all interfaces.

classofservice dot1p-mapping

M4250

M4350

This command maps an 802.1p priority to an internal traffic class. The *802.1p-priority* value can range from 0 to 7.

The *traffic-class* value depends on the switch model:

- For an M4250 series switch, the range is from 0 to 7.
- For an M4350 series switch, the range is from 0 to 6.

Format	<code>classofservice dot1p-mapping <i>802.1p-priority traffic-class</i></code>
Modes	Global Config Interface Config

no classofservice dot1p-mapping

This command maps each 802.1p priority to its default internal traffic class value.

Format	<code>no classofservice dot1p-mapping [<i>802.1p-priority</i>]</code>
Modes	Global Config Interface Config

classofservice ip-dscp-mapping

M4250

M4350

This command maps an IP DSCP value to an internal traffic class. The *ipdscp* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

The *traffic-class* value depends on the switch model:

- For an M4250 series switch, the range is from 0 to 7.
- For an M4350 series switch, the range is from 0 to 6.

Format	<code>classofservice ip-dscp-mapping ipdscp traffic-class</code>
Mode	Global Config

`no classofservice ip-dscp-mapping`

This command maps each IP DSCP value to its default internal traffic class value.

Format	<code>no classofservice ip-dscp-mapping</code>
Mode	Global Config

dante

M4250

M4350

This command sets the IGMP snooping querier interval to 30 seconds and configures the following class of service parameters:

- **`set igmp querier query-interval 30`**
- **`classofservice ip-dscp-mapping 46 5`**
- **`classofservice ip-dscp-mapping 48 5`**
- **`classofservice ip-dscp-mapping 56 6`**

Default	Disabled
Format	<code>dante</code>
Modes	Global Config

`no dante`

This command sets the following commands to the default values:

- **`set igmp querier query-interval`**
- **`classofservice ip-dscp-mapping`**

Format	<code>no dante</code>
Modes	Global Config

dante *vlan*

M4250

M4350

This command configures the following class of service parameters for all member ports of a particular VLAN:

- **classofservice trust ip-dscp**
- **cos-queue strict 5 6**

The *vlan* argument can be a VLAN from 1 to 4093.

This command applies the class of service parameters to all member ports of the specified VLAN. However, if a port is a member of multiple VLANs and one of those VLANs is configured for Dante but other VLANs are not, the Dante configuration takes precedence and is applied to the port.

Default	Disabled
Format	dante <i>vlan</i>
Modes	Global Config

no dante *vlan*

This command sets the following commands for all member ports of a particular VLAN to the default values:

- **classofservice trust**
- **cos-queue strict**

The *vlan* argument can be a VLAN from 1 to 4093.

Format	no dante <i>vlan</i>
Modes	Global Config

classofservice trust

M4250

M4350

This command sets the class of service trust mode of an interface or range of interfaces. You can set the mode to trust one of the Dot1p (802.1p), IP DSCP, or IP Precedence packet markings. You can also set the interface mode to untrusted. If you configure an interface to use Dot1p, the mode does not appear in the output of the show running-config command because Dot1p is the default.

Default	dot1p
Format	classofservice trust {dot1p ip-dscp untrusted}
Modes	Global Config Interface Config

no classofservice trust

This command sets the interface mode to the default value.

Format	no classofservice trust
Modes	Global Config Interface Config

cos-queue min-bandwidth

M4250

M4350

This command specifies the minimum transmission bandwidth (bw) guarantee for each interface queue on an interface, on a range of interfaces, or globally on all interfaces. The total number of queues supported per interface is depends on the switch model.

A value from 0-100 (percentage of link rate) must be specified for each supported queue, with 0 indicating no guaranteed minimum bandwidth. The sum of all values entered must not exceed 100.

Format	cos-queue min-bandwidth <i>bw-0</i> <i>bw-1</i> ... <i>bw-n</i>
Modes	Global Config Interface Config

no cos-queue min-bandwidth

This command restores the default for each queue's minimum bandwidth value.

Format	no cos-queue min-bandwidth
Modes	Global Config Interface Config

cos-queue random-detect

M4250

M4350

This command activates weighted random early discard (WRED) for each specified queue on the interface. Specific WRED parameters are configured using the **random-detect queue-parms** and the **random-detect exponential-weighting-constant** commands.

Format	<code>cos-queue random-detect queue-id-1 [queue-id-2 ... queue-id-n]</code>
Modes	Global Config Interface Config

When specified in Interface Config mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces.

At least one, but no more than n *queue-id* values are specified with this command. Duplicate *queue-id* values are ignored. Each *queue-id* value ranges from 0 to $(n-1)$, in which n is the total number of queues supported per interface. In the *queue-id-n* argument, the number $n = 7$ for M4250 series switches and $n = 6$ for M4350 series switches. The number corresponds to the number of supported queues (traffic classes).

no cos-queue random-detect

Use this command to disable WRED, thereby restoring the default tail drop operation for the specified queues on the interface.

Format	<code>no cos-queue random-detect queue-id-1 [queue-id-2 ... queue-id-n]</code>
Modes	Global Config Interface Config

cos-queue strict

M4250

M4350

This command activates the strict priority scheduler mode for each specified queue for an interface queue on an interface, a range of interfaces, or all interfaces.

At least one, but no more than n *queue-id* values are specified with this command. Duplicate *queue-id* values are ignored. Each *queue-id* value ranges from 0 to $(n-1)$, in which n is the total number of queues supported per interface. In the *queue-id-n* argument, the number $n = 7$ for M4250 series switches and $n = 6$ for M4350 series switches. The number corresponds to the number of supported queues (traffic classes).

Format	<code>cos-queue strict queue-id-1 [queue-id-2 ... queue-id-n]</code>

Modes	Global Config Interface Config

`no cos-queue strict`

This command restores the default weighted scheduler mode for each specified queue.

Format	<code>no cos-queue strict queue-id-1 [queue-id-2 ... queue-id-n]</code>

Modes	Global Config Interface Config

`random-detect exponential-weighting-constant`

M4250

M4350

This command is used to configure the WRED decay exponent for a CoS queue interface. The number argument is a value in the range of 0–15.

Format	<code>random-detect exponential-weighting-constant number</code>

Modes	Global Config Interface Config

`no random-detect exponential-weighting-constant`

Use this command to set the WRED decay exponent back to the default.

Format	<code>no random-detect exponential-weighting-constant</code>

Modes	Global Config Interface Config

`random-detect queue-parms`

M4250

M4350

This command is used to configure WRED parameters for each drop precedence level supported by a queue. It is used only when per-COS queue configuration is enabled (using the `cos-queue random-detect` command).

At least one, but no more than n `queue-id` values are specified with this command. Duplicate `queue-id` values are ignored. Each `queue-id` value ranges from 0 to $(n-1)$, in which n is the total number of queues supported per interface. In the `queue-id-n` argument,

the number $n = 7$ for M4250 series switches and $n = 6$ for M4350 series switches. The number corresponds to the number of supported queues (traffic classes).

The minimum and maximum threshold values can be configured in KB or percentage.

Each parameter is specified for each possible drop precedence (*color* of TCP traffic). The last precedence applies to all non-TCP traffic. For example, in a three-color system, three colors and one non-TCP precedence are specified for each parameter: green TCP, yellow TCP, red TCP, and non-TCP, respectively.

As an option, you can select ECN marking during congestion. When ECN is enabled, packets that are not marked as ECN capable are dropped when selected for discard by WRED.

Default	- WRED is not enabled for any CoS queue and ECN is not enabled for any CoS queue. - Minimum and maximum threshold units are percentage. The thresholds for each color and CoS queue are configured independently and can overlap. - WRED Minimum Threshold - Precedence level 0..... 40 - Precedence level 1..... 30 - Precedence level 2..... 20 - Precedence level 3..... 99 - WRED Maximum Threshold - Precedence level 0..... 100 - Precedence level 1..... 90 - Precedence level 2..... 80 - Precedence level 3..... 100 - WRED Drop Probability - Precedence level 0..... 10 - Precedence level 1..... 10 - Precedence level 2..... 10 - Precedence level 3..... 10
Format	<pre>random-detect queue-parms {queue-id-1 [queue-id-2 ... queue-id-n]} {units {KB percentage} {min-thresh minthresh-green minthresh-yellow minthresh-red minthresh-nontcp} {max-thresh max-thresh-green max-thresh-yellow max-thresh-red maxthresh-nontcp} {drop-prob dropprob-green dropprob-yellow dropprob-red dropprob-nontcp} [ecn]</pre>
Modes	Global Config Interface Config
Term	Definition
min-thresh	The minimum threshold the queue depth (as a percentage or KB) where WRED starts marking and dropping traffic. Specify the value for each color and for non-TCP.

Term	Definition
max-thresh	The maximum threshold is the queue depth (as a percentage or KB) above which WRED marks/drops all traffic. Specify the value for each color and for non-TCP.
drop-prob	The percentage probability (as a percentage or KB) that WRED will mark or drop a packet, when the queue depth is at the maximum threshold. Specify the value for each color and for non-TCP. (The drop probability increases linearly from 0 just before the minimum threshold, to this value at the maximum threshold, then goes to 100% for larger queue depths).

no random-detect queue-parms

Use this command to set the WRED configuration back to the default.

Format	<code>no random-detect queue-parms queue-id-1 [queue-id-2 ... queue-id-n]</code>
Modes	Global Config Interface Config

traffic-shape

M4250

M4350

This command specifies the maximum transmission bandwidth (*bw*) limit for the interface as a whole. The bandwidth values are from 0-100 in increments of 1. You can also specify this value for a range of interfaces or all interfaces. Also known as rate shaping, traffic shaping has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Format	<code>traffic-shape bw</code>
Modes	Global Config Interface Config

no traffic-shape

This command restores the interface shaping rate to the default value.

Format	<code>no traffic-shape</code>
Modes	Global Config Interface Config

show classofservice dot1p-mapping

M4250**M4350**

This command displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface.

The *unit/slot/port* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the 802.1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed. For more information, see [Voice VLAN Commands on page 566](#).

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	<code>show classofservice dot1p-mapping [unit/slot/port]</code>

Mode	Privileged EXEC

The following information is repeated for each user priority.

Term	Definition
User Priority	The 802.1p user priority value.
Traffic Class	The traffic class internal queue identifier to which the user priority value is mapped.

show classofservice ip-dscp-mapping

M4250**M4350**

This command displays the current IP DSCP mapping to internal traffic classes for the global configuration settings.

Format	<code>show classofservice ip-dscp-mapping</code>

Mode	Privileged EXEC

The following information is repeated for each user priority.

Term	Definition
IP DSCP	The IP DSCP value.
Traffic Class	The traffic class internal queue identifier to which the IP DSCP value is mapped.

show classofservice trust

M4250**M4350**

This command displays the current trust mode setting for a specific interface. The **unit/slot/port** parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If you specify an interface, the command displays the port trust mode of the interface. If you do not specify an interface, the command displays the most recent global configuration settings.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	<code>show classofservice trust [unit/slot/port]</code>

Mode	Privileged EXEC

Term	Definition
Class of Service Trust Mode	The the trust mode, which is either Dot1P, IP DSCP, or Untrusted.
Non-IP Traffic Class	(IP DSCP mode only) The traffic class used for non-IP traffic.
Untrusted Traffic Class	(Untrusted mode only) The traffic class used for all untrusted traffic.

show interfaces cos-queue

M4250**M4350**

This command displays the class-of-service queue configuration for the specified interface. The *unit/slot/port* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format	<code>show interfaces cos-queue [unit/slot/port]</code>

Mode	Privileged EXEC

Term	Definition
Interface Shaping Rate	The global interface shaping rate value.
WRED Decay Exponent	The global WRED decay exponent value.
Queue Id	An interface supports n queues numbered 0 to (n-1). The specific n value is platform dependent.
Minimum Bandwidth	The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This is a configured value.
Maximum Bandwidth	The maximum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This is a configured value.
Scheduler Type	Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This is a configured value.
Queue Management Type	The queue depth management technique used for this queue (tail drop).

If you specify the interface, the command also displays the following information.

Term	Definition
Interface	The <i>unit/slot/port</i> of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.
Interface Shaping Rate	The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth value(s) in effect for the interface. This is a configured value.
WRED Decay Exponent	The configured WRED decay exponent for a CoS queue interface.

show interfaces random-detect

M4250

M4350

This command displays the global WRED settings for each CoS queue. If you use the optional *unit/slot/port* argument, the command displays the WRED settings for each CoS queue on the specified interface. Valid interfaces include physical ports and port channels. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Explicit Congestion Notification (ECN) capability is also displayed.

The per CoS queue display for an interface displays the threshold, drop probability, and ECN capability per color in the order of green, yellow, red, and non-TCP.

Format `show interfaces random-detect [unit/slot/port]`

Mode Privileged EXEC

Term	Definition
Queue ID	The queue ID. An interface supports n queues numbered 0 to (n-1). The specific n value depends on the switch model.
WRED Minimum Threshold	The configured minimum threshold is the queue depth (as a percentage) where WRED starts marking and dropping traffic.
WRED Maximum Threshold	The configured maximum threshold is the queue depth (as a percentage) above which WRED marks or drops all traffic.
WRED Drop Probability	The configured percentage probability that WRED will mark or drop a packet when the queue depth is at the maximum threshold. (The drop probability increases linearly from 0 just before the minimum threshold to this value at the maximum threshold, then goes to 100% for larger queue depths).
ECN	Identifies if ECN is enabled.

Command example:

This output shows that ECN is enabled on CoS queues 0 and 1 with a minimum threshold of 40% for green colored packets, 30% for yellow colored packets, 20% for red colored packets and 100% for non-TCP packets.

```
(NETGEAR Switch)#show interfaces random-detect
```

Global Configuration

```
Queue ID..... 0
Threshold Units..... Percentage
WRED Minimum Threshold
  Precedence level 0..... 40
  Precedence level 1..... 30
  Precedence level 2..... 20
  Precedence level 3..... 99
WRED Drop Probability
  Precedence level 0..... 10
  Precedence level 1..... 10
  Precedence level 2..... 10
  Precedence level 3..... 10
ECN Enabled..... No
```

```
Queue ID..... 1
Threshold Units..... Percentage
WRED Minimum Threshold
  Precedence level 0..... 40
  Precedence level 1..... 30
```

Precedence level 2.....	20
Precedence level 3.....	99
WRED Drop Probability	
Precedence level 0.....	10
Precedence level 1.....	10
Precedence level 2.....	10
Precedence level 3.....	10
ECN Enabled.....	No

Differentiated Services Commands

This section describes the commands you use to configure QOS Differentiated Services (DiffServ).

You configure DiffServ in several stages by specifying three DiffServ components:

1. Class
 - a. Creating and deleting classes.
 - b. Defining match criteria for a class.
2. Policy
 - a. Creating and deleting policies
 - b. Associating classes with a policy
 - c. Defining policy statements for a policy/class combination
3. Service
 - a. Adding and removing a policy to/from an inbound interface

The DiffServ class defines the packet filtering criteria. The attributes of a DiffServ policy define the way the switch processes packets. You can define policy attributes on a per-class instance basis. The switch applies these attributes when a match occurs.

Packet processing begins when the switch tests the match criteria for a packet. The switch applies a policy to a packet when it finds a class match within that policy.

The following rules apply when you create a DiffServ class:

- Each class can contain a maximum of one referenced (nested) class
- Class definitions do not support hierarchical service policies

A class definition can contain a maximum of one reference to another class. You can combine the reference with other match criteria. The referenced class is truly a reference and not a copy since additions to a referenced class affect all classes that reference it. Changes to any class definition currently referenced by any other class must result in valid class definitions for all derived classes, otherwise the switch rejects the change. You can remove a class reference from a class definition.

The only way to remove an individual match criterion from an existing class definition is to delete the class and re-create it.

Note: The mark possibilities for policing include CoS, IP DSCP, and IP Precedence. While the latter two are only meaningful for IP packet types, CoS marking is allowed for both IP and non-IP packets, since it updates the 802.1p user priority field contained in the VLAN tag of the layer 2 packet header.

diffserv

M4250

M4350

This command sets the DiffServ operational mode to active. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format	diffserv
Mode	Global Config

no diffserv

This command sets the DiffServ operational mode to inactive. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format	no diffserv
Mode	Global Config

DiffServ Class Commands

Use the DiffServ class commands to define traffic classification. To classify traffic, you specify Behavior Aggregate (BA), based on DSCP and Multi-Field (MF) classes of traffic (name, match criteria)

This set of commands consists of class creation/deletion and matching, with the class match commands specifying Layer 3, Layer 2, and general match criteria. The class match criteria are also known as class rules, with a class definition consisting of one or more rules to identify the traffic that belongs to the class.

Note: After you create a class match criterion for a class, you cannot change or delete the criterion. To change or delete a class match criterion, you must delete and re-create the entire class.

The CLI command root is **class-map**.

class-map

M4250

M4350

This command defines a DiffServ class of type match-any or match-all. For the class type of **match-all**, when used without any match condition, this command enters the Class-Map Config mode.

The *class-map-name* is a case sensitive alphanumeric string from 1 to 31 characters uniquely identifying an existing DiffServ class. The *class-map-name* "default" is reserved.

The class type of **match-all** indicates all of the individual match conditions must be true for a packet to be considered a member of the class. This command may be used without specifying a class type to enter the Class-Map Config mode for an existing DiffServ class.

For the class type of **match-all**, the optional keywords **ipv4** and **ipv6** specify the Layer 3 protocol for this class. If not specified, this parameter defaults to IPv4. This maintains backward compatibility for configurations defined on systems before IPv6 match items were supported. The CLI mode is changed to Class-Map Config or IPv6-Class-Map Config when this command is successfully executed depending on whether you specify the **ipv4** or **ipv6** keyword.

For the class type of **match-any**, the CLI mode is changed to Class-Map Config when this command is successfully executed

Format	<code>class-map {match any <i>class-map-name</i> match-all <i>class-map-name</i> [ipv4 ipv6]}</code>
Mode	Global Config

no class-map

This command eliminates an existing DiffServ class. The *class-map-name* is the name of an existing DiffServ class. (The class name `default` is reserved and is not allowed here.) This command may be issued at any time; if the class is currently referenced by one or more policies or by any other class, the delete action fails.

Format	<code>no class-map <i>class-map-name</i></code>
Mode	Global Config

class-map rename

M4250**M4350**

This command changes the name of a DiffServ class. The *class-map-name* parameter is the name of an existing DiffServ class. The *new-class-map-name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class.

Default	none
Format	class-map rename <i>class-map-name</i> <i>new-class-map-name</i>
Mode	Global Config

match ethertype

M4250**M4350**

This command adds to the specified class definition a match condition based on the value of the ethertype. The **ethertype** value is specified as a *keyword* argument that can be one of the following types: **appletalk**, **arp**, **ibmsna**, **ipv4**, **ipv6**, **ipx**, **mplsmcast**, **mplsucast**, **netbios**, **novell**, **pppoe**, or **rarp** or as a *range* argument that represents an EtherType value in the range of 0x0600-0xFFFF.

Format	match ethertype { <i>keyword</i> <i>custom range</i> }
Mode	Class-Map Config Ipv6-Class-Map Config

match any

M4250**M4350**

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class.

Default	none
Format	match any
Mode	Class-Map Config Ipv6-Class-Map Config

match class-map

M4250

M4350

This command adds to the specified class definition the set of match conditions defined for another class. The *refclassname* is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Default	none
Format	match class-map <i>refclassname</i>
Mode	Class-Map Config Ipv6-Class-Map Config

The requirements for the **match class-map** command are as follows:

- The parameters *refclassname* and *class-map-name* can not be the same.
- Only one other class may be referenced by a class.
- Any attempts to delete the *refclassname* class while the class is still referenced by any *class-map-name* fail.
- The combined match criteria of *class-map-name* and *refclassname* must be an allowed combination based on the class type.
- Any subsequent changes to the *refclassname* class match criteria must maintain this validity, or the change attempt fails.
- The total number of class rules formed by the complete reference class chain (including both predecessor and successor classes) must not exceed a platform-specific maximum. In some cases, each removal of a refclass rule reduces the maximum number of available rules in the class definition by one.

no match class-map

This command removes from the specified class definition the set of match conditions defined for another class. The *refclassname* is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Format	no match class-map <i>refclassname</i>
Mode	Class-Map Config Ipv6-Class-Map Config

match cos

M4250**M4350**

This command adds to the specified class definition a match condition for the Class of Service value (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). The *value* argument can be from 0 to 7.

Default	none
Format	match cos <i>value</i>
Mode	Class-Map Config Ipv6-Class-Map Config

match secondary-cos

M4250**M4350**

This command adds to the specified class definition a match condition for the secondary Class of Service value (the inner 802.1Q tag of a double VLAN tagged packet).

The *value* argument can be from 0 to 7.

Default	none
Format	match secondary-cos <i>value</i>
Mode	Class-Map Config Ipv6-Class-Map Config

match destination-address mac

M4250**M4350**

This command adds to the specified class definition a match condition based on the destination MAC address of a packet. The *macaddr* parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The *macmask* parameter is a layer 2 MAC address bit mask, which need not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc).

Default	none
Format	match destination-address mac <i>macaddr macmask</i>
Mode	Class-Map Config Ipv6-Class-Map Config

match dstip

M4250

M4350

This command adds to the specified class definition a match condition based on the destination IP address of a packet. The *ipaddr* parameter specifies an IP address. The *ipmask* parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits.

Default	none
Format	match dstip <i>ipaddr ipmask</i>
Mode	Class-Map Config

match dstip6

M4250

M4350

This command adds to the specified class definition a match condition based on the destination IPv6 address of a packet.

Default	none
Format	match dstip6 <i>destination-ipv6-prefix/prefix-length</i>
Mode	Ipv6-Class-Map Config

match dstl4port

M4250

M4350

This command adds to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword, the value for *portkey* is one of the supported port name keywords. The *portkey* argument can be: **domain**, **echo**, **ftp**, **ftpdata**, **http**, **smtp**, **snmp**, **telnet**, **tftp**, or **www**. Each of these translates into its equivalent port number. To specify the match condition using a numeric notation, one layer 4 port number is required. The *port-number* argument is an integer from 0 to 65535.

Default	none
Format	match dstl4port { <i>portkey</i> <i>port-number</i> }
Mode	Class-Map Config Ipv6-Class-Map Config

match ip dscp

M4250

M4350

This command adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet, which is defined as the high-order six bits of the Service Type octet in the IP header (the low-order two bits are not checked).

The *dscpval* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **be**, **cs0**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **ef**.

Note: The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Default	none
Format	match ip dscp <i>dscpval</i>
Mode	Class-Map Config Ipv6-Class-Map Config

match ip precedence

M4250

M4350

This command adds to the specified class definition a match condition based on the value of the IP Precedence field in a packet, which is defined as the high-order three bits of the Service Type octet in the IP header (the low-order five bits are not checked). The precedence *value* argument is an integer from 0 to 7.

Note: The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Default	none
Format	match ip precedence <i>value</i>
Mode	Class-Map Config

match ip tos

M4250

M4350

This command adds to the specified class definition a match condition based on the value of the IP TOS field in a packet, which is defined as all eight bits of the Service Type octet in the IP header. The value of the *tosbits* argument is a two-digit hexadecimal number from 00 to ff. The value of *tosmask* argument is a two-digit hexadecimal number from 00 to ff. The *tosmask* denotes the bit positions in *tosbits* 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 *tosbits* value of a0 (hex) and a *tosmask* of a2 (hex).

Note: The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Note: This free form version of the IP DSCP/Precedence/ToS match specification gives you complete control when specifying which bits of the IP Service Type field are checked.

Default	none
Format	match ip tos <i>tosbits tosmask</i>
Mode	Class-Map Config

match ip6flowlbl

M4250

M4350

Use this command to enter an IPv6 flow label value. The *value* argument can be in the range of 0–1048575.

Default	none
Format	match ip6flowlbl label <i>value</i>
Mode	IPv6-Class-Map Config

match protocol

M4250**M4350**

This command adds to the specified class definition a match condition based on the value of the IP Protocol field in a packet using a single keyword notation or a numeric value notation.

To specify the match condition using a single keyword notation, the value for *protocol-name* is one of the supported protocol name keywords.

For IPv4, the supported options are **icmp**, **igmp**, **ip**, **tcp**, **udp**, and **gre**. A value of **ip** matches all protocol number values.

For IPv6, the supported options are **ipv6**, **icmpv6**, **tcp**, and **udp**.

To specify the match condition using a numeric value notation, the protocol *number* argument is a standard value assigned by IANA and is interpreted as an integer from 0 to 255.

Note: This command does not validate the protocol number value against the current list defined by IANA.

Default	none
Format	match protocol { <i>protocol-name</i> <i>number</i> none}
Mode	Class-Map Config Ipv6-Class-Map Config

match source-address mac

M4250**M4350**

This command adds to the specified class definition a match condition based on the source MAC address of a packet. The *address* parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The *macmask* parameter is a layer 2 MAC address bit mask, which may not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (that is, ff:07:23:ff:fe:dc).

Default	none
Format	match source-address mac <i>address macmask</i>
Mode	Class-Map Config Ipv6-Class-Map Config

match srcip

M4250**M4350**

This command adds to the specified class definition a match condition based on the source IP address of a packet. The *ipaddr* parameter specifies an IP address. The *ipmask* parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits.

Default	none
Format	match srcip <i>ipaddr ipmask</i>
Mode	Class-Map Config

match srcip6

M4250**M4350**

This command adds to the specified class definition a match condition based on the source IP address of a packet.

Default	none
Format	match srcip6 <i>source-ipv6-prefix/prefix-length</i>
Mode	Ipv6-Class-Map Config

match srcl4port

M4250**M4350**

This command adds to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword notation, the value for *portkey* is one of the supported port name keywords (listed below). The currently supported *portkey* values are: **domain**, **echo**, **ftp**, **ftpdata**, **http**, **smtp**, **snmp**, **telnet**, **tftp**, and **www**. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.

To specify the match condition as a numeric value, one layer 4 port number is required. The *port-number* argument is an integer from 0 to 65535.

Default	none
Format	match srcl4port { <i>portkey</i> <i>port-number</i> }
Mode	Class-Map Config Ipv6-Class-Map Config

match vlan

M4250

M4350

This command adds to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field (the only tag in a single tagged packet or the first or outer tag of a double VLAN tagged packet). The *vlan-id* argument is an integer from 0 to 4093.

Default	none
Format	match vlan <i>vlan-id</i>
Mode	Class-Map Config Ipv6-Class-Map Config

match secondary-vlan

M4250

M4350

This command adds to the specified class definition a match condition based on the value of the layer 2 secondary VLAN Identifier field (the inner 802.1Q tag of a double VLAN tagged packet). The secondary *vlan-id* argument is an integer from 0 to 4093.

Default	none
Format	match secondary-vlan <i>vlan-id</i>
Mode	Class-Map Config Ipv6-Class-Map Config

DiffServ Policy Commands

Use the DiffServ policy commands to specify traffic conditioning actions, such as policing and marking, to apply to traffic classes

Use the policy commands to associate a traffic class that you define by using the class command set with one or more QoS policy attributes. Assign the class/policy association to an interface to form a service. Specify the policy name when you create the policy.

Each traffic class defines a particular treatment for packets that match the class definition. You can associate multiple traffic classes with a single policy. When a packet satisfies the conditions of more than one class, preference is based on the order in which you add the classes to the policy. The first class you add has the highest precedence.

This set of commands consists of policy creation and deletion, class addition and removal, and setting individual policy attributes.

Note: The only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and re-add it to the policy. The values associated with an existing policy attribute can be changed without removing the class instance.

The CLI command root is **policy-map**.

policy-map

M4250

M4350

This command establishes a new DiffServ policy. The *polycyname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy. The type of policy is specific to the inbound traffic direction as indicated by the **in** parameter, or the outbound traffic direction as indicated by the **out** parameter, respectively.

Note: The CLI mode is changed to Policy-Map Config when this command is successfully executed.

Format	<code>policy-map <i>polycyname</i> {in out}</code>

Mode	Global Config

no policy-map

This command removes an existing DiffServ policy. The *polycyname* parameter is the name of an existing DiffServ policy. If the policy is currently referenced by one or more interface service attachments, you cannot remove the policy map.

Format	<code>no policy-map <i>polycyname</i></code>

Mode	Global Config

policy-map rename

M4250**M4350**

This command changes the name of a DiffServ policy. The *polycyname* is the name of an existing DiffServ class. The *newpolycyname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy.

Format	<code>policy-map rename <i>polycyname</i> <i>newpolycyname</i></code>

Mode	Global Config

class

M4250**M4350**

This command creates an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements. The *classname* argument must be the name of an existing DiffServ class.

Note: This command causes the specified policy to create a reference to the class definition.

Note: The CLI mode is changed to Policy-Class-Map Config when this command is successfully executed.

Format	<code>class <i>classname</i></code>

Mode	Policy-Map Config

no class

This command deletes the instance of a particular class and its defined treatment from the specified policy. The *classname* argument is the name of an existing DiffServ class.

Note: This command removes the reference to the class definition for the specified policy.

Format	<code>no class <i>classname</i></code>

Mode	Policy-Map Config

assign-queue

M4250

M4350

This command modifies the queue ID to which the associated traffic stream is assigned. The *queueid* is an integer from 0 to $n-1$, in which n is the number of egress queues supported by the switch. The range is from 0 to 7.

Format	<code>assign-queue <i>queueid</i></code>

Mode	Policy-Class-Map Config

Incompatibilities	Drop

drop

M4250

M4350

This command specifies that all packets for the associated traffic stream must be dropped at ingress.

Format	<code>drop</code>

Mode	Policy-Class-Map Config

Incompatibilities	Assign Queue, Mark (all forms), Mirror, Police, Redirect

mirror

M4250

M4350

This command specifies that all incoming packets for the associated traffic stream are copied to a specific egress interface (physical port or LAG).

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	<code>mirror {unit/slot/port lag lag-intf-num}</code>

Mode	Policy-Class-Map Config

Incompatibilities	Drop, Redirect

redirect

M4250

M4350

This command specifies that all incoming packets for the associated traffic stream are redirected to a specific egress interface (physical port or port-channel).

Format	<code>redirect {unit/slot/port lag lag-intf-num}</code>

Mode	Policy-Class-Map Config

Incompatibilities	Drop, Mirror

conform-color

M4250

M4350

Use this command to enable color-aware traffic policing and define the conform-color class map and the color exceed mode.

Use this command in conjunction with the police command where the fields for the conform level are specified. The *class-map-name* argument is the name of an existing DiffServ class map.

Note: You can use this command only after you specify a police command for the policy-class instance.

Format	<code>conform-color class-map-name [exceed-color class-map-name]</code>

Mode	Policy-Class-Map Config

mark cos

M4250

M4350

This command marks all packets for the associated traffic stream with the specified class of service (CoS) value in the priority field of the 802.1p header (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). If the packet does

not already contain this header, one is inserted. The CoS *value* argument is an integer from 0 to 7.

Default	1
Format	<code>mark-cos value</code>
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

mark ip-dscp

M4250

M4350

This command marks all packets for the associated traffic stream with the specified IP DSCP value. The *dscpval* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **be**, **cs0**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **ef**.

Format	<code>mark ip-dscp dscpval</code>
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police

mark ip-precedence

M4250

M4350

This command marks all packets for the associated traffic stream with the specified IP Precedence value. The IP Precedence *value* argument is an integer from 0 to 7.

Note: This command may not be used on IPv6 classes. IPv6 does not have a precedence field.

Format	<code>mark ip-precedence value</code>
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police
Policy Type	In

police-simple

M4250**M4350**

This command is used to establish the traffic policing style for the specified class. The simple form of the **police** command uses a single data rate and burst size, resulting in two outcomes: conform and violate.

The conforming data rate is specified in kilobits-per-second (Kbps) as an integer from 1 to 4294967295 or a percentage from 1 to 100. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128.

Just must set the conform action and violate action. For each outcome, the only possible actions are **drop**, **set-cos-transmit**, **set-dscp-transmit**, **set-prec-transmit**, or **transmit**. In this simple form of the **police** command, the conform action defaults to transmit and the violate action defaults to drop. These actions can be set with this command after you configure the style:

- For **set-cos-transmit** an 802.1p priority value is required and is specified as an integer from 0-7.
- For **set-dscp-transmit**, a value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **be**, **cs0**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **ef**.
- For **set-prec-transmit**, an IP Precedence value is required and is specified as an integer from 0-7.

Format	<pre>police-simple {rate-kbps 1-4294967295 1-128 rate-percent 1-100 1-128} {conform-action {drop set-cos-transmit 0-7 set-prec-transmit 0-7 set-dscp-transmit 0-63 transmit}} {violate-action {drop set-cos-transmit 0-7 set-prec-transmit 0-7 set-dscp-transmit 0-63 transmit}}</pre>

Mode	Policy-Class-Map Config

Incompatibilities	Drop, Mark (all forms)

Command example:

```
(NETGEAR Switch) (Config-policy-classmap)#police-simple 1 128 conform-action transmit
violate-action drop
```

police-single-rate

M4250**M4350**

This command is the single-rate form of the **police** command and is used to establish the traffic policing style for the specified class.

The conforming data rate is specified in kilobits-per-second (Kbps) as an integer from 1 to 4294967295 or a percentage from 1 to 100. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128. Unlike for the **policy-simple** command, for the **police-single-rate** command, you must also set the excess burst size, which is specified in kilobytes (KB) and is an integer from 1 to 128.

Just must set the confirm action, exceed action, and violate action. For each outcome, the only possible actions are **drop**, **set-cos-transmit**, **set-dscp-transmit**, **set-prec-transmit**, or **transmit**. In this simple form of the **police** command, the conform action defaults to transmit and the violate action defaults to drop. These actions can be set with this command after you configure the style:

- For **set-cos-transmit** an 802.1p priority value is required and is specified as an integer from 0-7.
- For **set-dscp-transmit**, a value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **be**, **cs0**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **ef**.
- For **set-prec-transmit**, an IP Precedence value is required and is specified as an integer from 0-7.

Format	<pre>police-single-rate {rate-kbps 1-4294967295 1-128 1-128 rate-percent 1-100 1-128 1-128} {conform-action {drop set-cos-transmit 0-7 set-prec-transmit 0-7 set-dscp-transmit 0-63 transmit}} {exceed-action {drop set-cos-transmit 0-7 set-prec-transmit 0-7 set-dscp-transmit 0-63 transmit}} {violate-action {drop set-cos-transmit 0-7 set-prec-transmit 0-7 set-dscp-transmit 0-63 transmit}}</pre>

Mode	Policy-Class-Map Config

police-two-rate

M4250

M4350

This command is the two-rate form of the **police** command and is used to establish the traffic policing style for the specified class.

This command is the single-rate form of the **police** command and is used to establish the traffic policing style for the specified class.

The conforming data rate is specified in kilobits-per-second (Kbps) as an integer from 1 to 4294967295 or a percentage from 1 to 100. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128. Unlike for the **policy-simple** command, for the **police-two-rate** command, you must also set the peak data rate, which is specified as an integer from 1 to 4294967295 or a percentage from 1 to 100, and you must also set the excess burst size, which is specified in kilobytes (KB) and is an integer from 1 to 128.

Just must set the confirm action, exceed action, and violate action. For each outcome, the only possible actions are **drop**, **set-cos-transmit**, **set-dscp-transmit**,

set-prec-transmit, or **transmit**. In this simple form of the **police** command, the conform action defaults to transmit and the violate action defaults to drop. These actions can be set with this command after you configure the style:

- For **set-cos-transmit** an 802.1p priority value is required and is specified as an integer from 0-7.
- For **set-dscp-transmit**, a value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **be**, **cs0**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **ef**.
- For **set-prec-transmit**, an IP Precedence value is required and is specified as an integer from 0-7.

Format	<pre>police-two-rate {rate-kbps 1-4294967295 1-128 1-4294967295 1-128 rate-percent 1-100 1-128 1-100 1-128} {conform-action {drop set-cos-transmit 0-7 set-prec-transmit 0-7 set-dscp-transmit 0-63 transmit}} {exceed-action {drop set-cos-transmit 0-7 set-prec-transmit 0-7 set-dscp-transmit 0-63 transmit}} {violate-action {drop set-cos-transmit 0-7 set-prec-transmit 0-7 set-dscp-transmit 0-63 transmit}}</pre>

Mode	Policy-Class-Map Config

DiffServ Service Commands

Use the DiffServ service commands to assign a DiffServ traffic conditioning policy, which you specified by using the policy commands, to an interface in the incoming direction

The service commands attach a defined policy to a directional interface. You can assign only one policy at any one time to an interface in the inbound direction. DiffServ is not used in the outbound direction.

This set of commands consists of service addition or removal.

The CLI command root is **service-policy**.

service-policy

M4250

M4350

This command attaches a policy to an interface in the inbound direction as indicated by the **in** parameter, or the outbound direction as indicated by the **out** parameter, respectively. The *polycyname* parameter must be the name of an existing DiffServ policy. This command causes a service to create a reference to the policy.

Note: This command effectively enables DiffServ on an interface in the inbound direction. There is no separate interface administrative mode command for DiffServ.

Note: This command fails if any attributes within the policy definition exceed the capabilities of the interface. Once a policy is successfully attached to an interface, any attempt to change the policy definition, that would result in a violation of the interface capabilities, causes the policy change attempt to fail.

Format	<code>service-policy {in out} <i>polycyname</i></code>

Modes	Global Config Interface Config

Note: Each interface can have one policy attached.

no service-policy

This command detaches a policy from an interface in the inbound direction as indicated by the **in** parameter, or the outbound direction as indicated by the **out** parameter, respectively. The *polycyname* parameter is the name of an existing DiffServ policy.

Note: This command causes a service to remove its reference to the policy. This command effectively disables DiffServ on an interface in the inbound direction or an interface in the outbound direction. There is no separate interface administrative 'mode' command for DiffServ.

Format	<code>no service-policy {in out} <i>polycyname</i></code>

Modes	Global Config Interface Config

DiffServ Show Commands

Use the DiffServ show commands to display configuration and status information for classes, policies, and services. You can display DiffServ information in summary or detailed formats. The status information is only shown when the DiffServ administrative mode is enabled.

show class-map

M4250

M4350

This command displays all configuration information for the specified class. The *class-name* is the name of an existing DiffServ class.

Format	show class-map <i>class-name</i>
Modes	Privileged EXEC User EXEC

If the class-name is specified the following fields are displayed.

Term	Definition
Class Name	The name of this class.
Class Type	A class type of all means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
Class Layer3 Protocol	The Layer 3 protocol for this class. Possible values are IPv4 and IPv6.
Match Criteria	The Match Criteria fields are only displayed if they have been configured. Not all platforms support all match criteria values. They are displayed in the order entered by the user. The fields are evaluated in accordance with the class type. The possible Match Criteria fields are: Destination IP Address, Destination Layer 4 Port, Destination MAC Address, Ethertype, Source MAC Address, VLAN, Class of Service, Every, IP DSCP, IP Precedence, IP TOS, Protocol Keyword, Reference Class, Source IP Address, and Source Layer 4 Port.
Values	The values of the Match Criteria.

If you do not specify the Class Name, this command displays a list of all defined DiffServ classes. The following fields are displayed.

Term	Definition
Class Name	The name of this class. (Note that the order in which classes are displayed is not necessarily the same order in which they were created.)

Term	Definition
Class Type	A class type of all means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
Ref Class Name	The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

show diffserv

M4250

M4350

This command displays the DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables.

Format `show diffserv`

Mode Privileged EXEC

Term	Definition
DiffServ Admin mode	The current value of the DiffServ administrative mode.
Class Table Size Current/Max	The current and maximum number of entries (rows) in the Class Table.
Class Rule Table Size Current/Max	The current and maximum number of entries (rows) in the Class Rule Table.
Policy Table Size Current/Max	The current and maximum number of entries (rows) in the Policy Table.
Policy Instance Table Size Current/Max	The current and maximum number of entries (rows) in the Policy Instance Table.
Policy Instance Table Max Current/Max	The current and maximum number of entries (rows) for the Policy Instance Table.
Policy Attribute Table Max Current/Max	The current and maximum number of entries (rows) for the Policy Attribute Table.
Service Table Size Current/Max	The current and maximum number of entries (rows) in the Service Table.

show policy-map

M4250

M4350

This command displays all configuration information for the specified policy. The *polycyname* is the name of an existing DiffServ policy.

Format `show policy-map [polycyname]`

Mode Privileged EXEC

If the Policy Name is specified the following fields are displayed.

Term	Definition
Policy Name	The name of this policy.
Policy Type	The policy type (only inbound policy definitions are supported for this platform.)
Class Members	The class that is a member of the policy.

The following information is repeated for each class associated with this policy (only those policy attributes actually configured are displayed).

Term	Definition
Assign 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.
Class Name	The name of this class.
Committed Burst Size (KB)	The committed burst size, used in simple policing.
Committed Rate (Kbps)	The committed rate, used in simple policing.
Conform Action	The current setting for the action taken on a packet considered to conform to the policing parameters. This is not displayed if policing is not in use for the class under this policy.
Conform Color Mode	The current setting for the color mode. Policing 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.
Conform CoS	The CoS mark value if the conform action is set-cos-transmit.
Conform DSCP Value	The DSCP mark value if the conform action is set-dscp-transmit.
Conform IP Precedence Value	The IP Precedence mark value if the conform action is set-prec-transmit.
Drop	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.
Exceed Action	The action taken on traffic that exceeds settings that the network administrator specifies.
Exceed Color Mode	The current setting for the color of exceeding traffic that the user may optionally specify.
Mark CoS	The class of service value that is set in the 802.1p header of inbound packets. This is not displayed if the mark cos was not specified.
Mark CoS as Secondary CoS	The secondary 802.1p priority value (second/inner VLAN tag. Same as CoS (802.1p) marking, but the dot1p value used for remarking is picked from the dot1p value in the secondary (i.e. inner) tag of a double-tagged packet.
Mark IP DSCP	The mark/re-mark value used as the DSCP for traffic matching this class. This is not displayed if mark ip description is not specified.

Term	Definition
Mark IP Precedence	The mark/re-mark value used as the IP Precedence for traffic matching this class. This is not displayed if mark ip precedence is not specified.
Mirror	Copies a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment.
Non-Conform Action	The current setting for the action taken on a packet considered to not conform to the policing parameters. This is not displayed if policing not in use for the class under this policy.
Non-Conform COS	The CoS mark value if the non-conform action is set-cos-transmit.
Non-Conform DSCP Value	The DSCP mark value if the non-conform action is set-dscp-transmit.
Non-Conform IP Precedence Value	The IP Precedence mark value if the non-conform action is set-prec-transmit.
Peak Rate	Guarantees a committed rate for transmission, but also transmits excess traffic bursts up to a user-specified peak rate, with the understanding that a downstream network element (such as the next hop's policer) might drop this excess traffic. Traffic is held in queue until it is transmitted or dropped (per type of queue depth management.) Peak rate shaping can be configured for the outgoing transmission stream for an AP traffic class (although average rate shaping could also be used.)
Peak Burst Size	(PBS). The network administrator can set the PBS as a means to limit the damage expedited forwarding traffic could inflict on other traffic (e.g., a token bucket rate limiter) Traffic that exceeds this limit is discarded.
Policing Style	The style of policing, if any, used (simple).
Redirect	Forces a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment.

If the Policy Name is not specified this command displays a list of all defined DiffServ policies. The following fields are displayed.

Term	Definition
Policy Name	The name of this policy. (The order in which the policies are displayed is not necessarily the same order in which they were created.)
Policy Type	The policy type (Only inbound is supported).
Class Members	List of all class names associated with this policy.

Command example:

The following example includes the mark-cos-as-sec-cos option that is specified in the policy action.

```
(NETGEAR Switch) #show policy-map p1
Policy Name..... p1
Policy Type..... In
```

```
Class Name..... c1
Mark CoS as Secondary CoS..... Yes
```

Command example:

The following example includes the mark-cos-as-sec-cos action that is used in the policing (simple-police, police-single-rate, police two-rate) command.

```
(NETGEAR Switch) #show policy-map p2
Policy Name..... p2
Policy Type..... In
Class Name..... c2
Policing Style..... Police Two Rate
Committed Rate..... 1
Committed Burst Size..... 1
Peak Rate..... 1
Peak Burst Size..... 1
Conform Action..... Mark CoS as Secondary CoS
Exceed Action..... Mark CoS as Secondary CoS
Non-Conform Action..... Mark CoS as Secondary CoS
Conform Color Mode..... Blind
Exceed Color Mode..... Blind
```

show diffserv service**M4250****M4350**

This command displays policy service information for the specified interface and direction. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The direction parameter is required.

Format	<code>show diffserv service unit/slot/port {in out}</code>
Mode	Privileged EXEC

Term	Definition
DiffServ Admin Mode	The current setting of the DiffServ administrative mode. An attached policy is only in effect on an interface while DiffServ is in an enabled mode.
Interface	The interface.
Direction	The traffic direction of this interface service.

Term	Definition
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.
Policy Details	Attached policy details, for which the content is identical to that described for the show policy-map <i>polycymapname</i> command. (The content is not repeated here for brevity).

show diffserv service brief

M4250

M4350

This command displays all interfaces in the system to which a DiffServ policy has been attached. The direction parameter is optional.

Format	<code>show diffserv service brief [in out]</code>
Mode	Privileged EXEC

Term	Definition
DiffServ Mode	The current setting of the DiffServ administrative mode. An attached policy is only active on an interface while DiffServ is in an enabled mode.

The following information is repeated for interface and direction (only those interfaces configured with an attached policy are shown).

Term	Definition
Interface	The interface.
Direction	The traffic direction of this interface service.
OperStatus	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

show policy-map interface

M4250

M4350

This command displays policy-oriented statistics information for the specified interface and direction.

To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

You can also use **lag** *lag-intf-num* to specify the LAG interface, in which *lag-intf-num* is the LAG port number.

The direction parameter is required.

Note: This command functions only if the DiffServ administrative mode is enabled.

Format	<code>show policy-map interface unit/slot/port {in out}</code>
Mode	Privileged EXEC
Term	Definition
Interface	The interface.
Direction	The traffic direction of this interface service.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

The following information is repeated for each class instance within this policy:

Term	Definition
Class Name	The name of this class instance.
In Discarded Packets	A count of the packets discarded for this class instance for any reason due to DiffServ treatment of the traffic class.

show service-policy

M4250

M4350

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction. The direction parameter is required.

Format	<code>show service-policy {in out}</code>
Mode	Privileged EXEC

The following information is repeated for each interface and direction (only those interfaces configured with an attached policy are shown):

Term	Definition
Interface	The interface.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface.

MAC Access Control List Commands

This section describes the commands you use to configure MAC Access Control List (ACL) settings. MAC ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to MAC ACLs:

- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per MAC ACL is hardware dependent.

mac access-list extended

M4250

M4350

This command creates a MAC Access Control List (ACL) identified by *name*, consisting of classification fields defined for the Layer 2 header of an Ethernet frame. The *name* parameter can include alphabetic, numeric, dash, dot and, underscore characters only, and must start with a letter. The size of the name string must be less than or equal to 255 characters.

If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing MAC ACL.

Note: The CLI mode changes to Mac-Access-List Config mode when you successfully execute this command.

Format	mac access-list extended <i>name</i>
Mode	Global Config

no mac access-list extended

This command deletes a MAC ACL identified by *name* from the system.

Format	no mac access-list extended <i>name</i>
Mode	Global Config

mac access-list extended rename

M4250

M4350

This command changes the name of a MAC Access Control List (ACL). The *name* parameter is the name of an existing MAC ACL. The *newname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

This command fails if a MAC ACL by the name *newname* already exists.

Format	mac access-list extended rename <i>name newname</i>
Mode	Global Config

mac access-list resequence

M4250

M4350

Use this command to renumber the sequence of the entries for a specified MAC access list with a specified increment value, starting from a specified sequence number. That is, with this command you can change the sequence numbers of ACL rules in the ACL and, therefore, change the order in which entries are applied. This command is not saved in the startup configuration and does not display in the running configuration.

Note: If the generated sequence number exceeds the maximum sequence number, the ACL rule creation fails and an informational message displays.

Default	10
Format	mac access-list resequence <i>name starting-sequence-number increment</i>
Mode	Global Config

Parameter	Description
name	The name of the access control list.
id	The ID of the access control list.

Parameter	Description
starting-sequence-number	The sequence number from which to start the renumbering. The range is 1–2147483647. The default is 10.
increment	The value with which the sequence numbers must be incremented. The range is 1–2147483647. The default is 10.

[sequence-number] {deny | permit} (MAC ACL)

M4250

M4350

This command creates a new rule for the current MAC access list. Each rule is appended to the list of configured rules for the list. A rule may either deny or permit traffic according to the specified classification fields.

At a minimum, the source (*srcmac*) and destination (*dstmac*) MAC value must be specified, each of which may be substituted using the keyword *any* to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

Format	[sequence-number] {deny permit} {srcmac any} {dstmac any bpdu} [ethertypekey 0x0600-0xFFFF] [vlan {eq 0-4095}] [cos 0-7] [[log] [time-range time-range-name] [assign-queue queue-id]] [{mirror redirect} unit/slot/port] [rate-limit rate burst-size]
Mode	Mac-Access-List Config

Note: An implicit **deny all** MAC rule always terminates the access list.

Usage guidelines

The sequence number specifies the sequence number for the ACL rule. Either you define the sequence number or is it is generated.

If no sequence number exists for a rule, a sequence number that is 10 greater than the last sequence number in the ACL is used and the rule is placed at the end of the list. If this is the first ACL rule in the ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the creation of the ACL rule fails. You cannot create a rule that duplicates an already existing one and you cannot configure a rule with a sequence number that is already used for another rule.

For example, if you add new ACL rule to the ACL without specifying a sequence number, the rule is placed at the bottom of the list. By changing the sequence number, you can move the ACL rule to a different position in the ACL.

The **any** keyword configure a match condition for all the destination MAC addresses in the destination MAC address field. The **bpdu** keyword configures a match condition on any Bridge Protocol Data Unit (BPDU) destination MAC address.

You can specify the Ethertype as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported *ethertypekey* values are: **appletalk**, **arp**, **ibmsna**, **ipv4**, **ipv6**, **ipx**, **mplsmcast**, **mplsucast**, **netbios**, **novell**, **pppoe**, and **rarp**. Each of these translates into its equivalent Ethertype value(s).

Table 12. Ethertype keyword and 4-digit hexadecimal value

Ethertype Keyword	Corresponding Value
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5
ipv4	0x0800
ipv6	0x86DD
ipx	0x8037
mplsmcast	0x8848
mplsucast	0x8847
netbios	0x8191
novell	0x8137, 0x8138
pppoe	0x8863, 0x8864
rarp	0x8035

The **vlan** and **cos** parameters refer to the VLAN identifier and 802.1p user priority fields, respectively, of the VLAN tag. For packets containing a double VLAN tag, this is the first (or outer) tag.

The **time-range** parameter allows imposing time limitation on the MAC ACL rule as defined by the parameter *time-range-name*. If a time range with the specified name does not exist and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see [Time Range Commands for Time-Based ACLs on page 1349](#).

The **assign-queue** parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed *queue-id* value is 0-(*n*-1), in which *n* is the number of user configurable queues available for the hardware platform:

- M4250 series switch: from 0 to 7.
- M4350 series switch: from 0 to 6.

The **assign-queue** parameter is valid only for a **permit** rule.

The `mirror` parameter allows the traffic matching this rule to be copied to the specified interface, while the `redirect` parameter allows the traffic matching this rule to be forwarded to the specified interface. The `assign-queue` and `redirect` parameters are only valid for a `permit` rule. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument `slot/port`.
- For an M4350 series switch, use the argument `unit/slot/port`, as shown in the command format.

Note: The special command form `{deny | permit} any any` is used to match all Ethernet layer 2 packets, and is the equivalent of the IP access list “match every” rule.

The `permit` command's optional attribute `rate-limit` allows you to permit only the allowed rate of traffic as per the configured `rate` in kbps from 1-4294967295, and `burst-size` in kbytes from 1-128.

Command example:

```
(NETGEAR Switch) (Config)#mac access-list extended mac1
(NETGEAR Switch) (Config-mac-access-list)#permit 00:00:00:00:aa:bb ff:ff:ff:ff:00:00 any
rate-limit 32 16
(NETGEAR Switch) (Config-mac-access-list)#exit
```

`no sequence-number` (MAC ACL)

Use this command to remove the ACL rule with the specified sequence number from the ACL.

Format	<code>no sequence-number</code>

Modes	MAC-Access-List Config

`mac access-group`

M4250

M4350

This command either attaches a specific MAC Access Control List (ACL) identified by `name` to an interface or range of interfaces, or associates it with a VLAN ID in a specified direction. The `name` parameter must be the name of an existing MAC ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other mac access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified mac access list replaces the currently attached mac access list using that sequence number. If the sequence number is not specified for this

command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The **vlan** keyword and *vlan-id* argument are valid only in the Global Config mode. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

An optional **control-plane** is specified to apply the MAC ACL on CPU port. The control packets like BPDU are also dropped because of the implicit deny all rule added to the end of the list. To overcome this, permit rules must be added to allow the control packets.

Note: The **control-plane** keyword is available only in Global Config mode.
Depending on the platform, the out option might not be available.

Format	<code>mac access-group name {{control-plane in out} vlan vlan-id {in out}}</code> <code>[sequence 1-4294967295]</code>
Modes	Global Config Interface Config
Parameter	Description
name	The name of the Access Control List.
vlan-id	A VLAN ID associated with a specific IP ACL.
sequence	A optional sequence number that indicates the order of this IP access list relative to the other IP access lists already assigned to this interface and direction. The range is 1 to 4294967295.

```
(NETGEAR Switch) (Config) #mac access-group mac1 control-plane
```

no mac access-group

This command removes a MAC ACL identified by *name* from the interface in a specified direction.

Format	<code>no mac access-group name {{control-plane in out} vlan vlan-id {in out}}</code>
Modes	Global Config Interface Config

Command example:

```
(NETGEAR Switch) (Config) #no mac access-group mac1 control-plane
```

remark

M4250

M4350

This command adds a new comment to an ACL rule.

Use the **remark** keyword to add comments (remarks) to an ACL rule entry that belongs to an IPv4, IPv6, MAC, or ARP ACL. You can add up to 10 * (maximum number of ACL rules per list) remarks per ACL and up to 10 remarks per ACL rule. For all QoS ACLs (IPv4, IPv6, and MAC ACLs) together, you can up to add 2 * (maximum number of ACL rules).

You can only add a remark before you create a rule. Remarks are associated with the ACL rule that is created immediately after the remarks are created. If you add 10 remarks, each one is linked to the rule that is created immediately afterwards.

If the ACL rule is removed, the associated remarks are also deleted. Remarks are shown only in output of the **show running-config** command and not in the output of the **show [ip | mac | arp] access-lists** command.

The total length of a single remark cannot exceed 100 characters. A remark can contain characters in the ranges A-Z, a-z, and 0-9, and special characters such as a space, hyphen, and underscore.

Format	<code>remark comment</code>
Modes	IPv4-Access-List Config IPv6-Access-List-Config MAC-Access-List Config ARP-Access-List Config

Command example:

```
(Config)#arp access-list new
(Config-arp-access-list)#remark "test1"
(Config-arp-access-list)#permit ip host 1.1.1.1 mac host 00:01:02:03:04:05
(Config-arp-access-list)#remark "test1"
(Config-arp-access-list)#remark "test2"
(Config-arp-access-list)#remark "test3"
(Config-arp-access-list)#permit ip host 1.1.1.2 mac host 00:03:04:05:06:07
(Config-arp-access-list)#permit ip host 2.1.1.2 mac host 00:03:04:05:06:08
(Config-arp-access-list)#remark "test4"
(Config-arp-access-list)#remark "test5"
(Config-arp-access-list)#permit ip host 2.1.1.3 mac host 00:03:04:05:06:0
```

no remark

Use this command to remove a remark from an ACL.

When you enter this command, the first occurrence of the remark in the ACL is deleted. Each time that you repeat the command with the same remark, the remark is deleted from the next ACL rule with which the remark is associated.

If all occurrences of the remark are deleted and you enter the command, an error message displays.

Format	<code>no remark comment</code>
Modes	IPv4-Access-List Config IPv6-Access-List-Config MAC-Access-List Config ARP-Access-List Config

show mac access-lists

M4250

M4350

This command displays summary information for all MAC access lists and shows the number of packets that match a configured ACL rule within an ACL (referred to as ACL hit count).

To view more detailed information about a specific access list, specify the ACL name that is used to identify the MAC ACL.

Note: The command output varies based on the match criteria configured within the rules of an ACL. The next table show fields that can be displayed in the command output.

Format	<code>show mac access-lists [name]</code>
Mode	Privileged EXEC
Term	Definition
Rule Number	The ordered rule number identifier defined within the MAC ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Source MAC Address	The source MAC address for this rule.
Source MAC Mask	The source MAC mask for this rule.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Destination MAC Address	The destination MAC address for this rule.
Ethertype	The Ethertype keyword or custom value for this rule.
VLAN ID	The VLAN identifier value or range for this rule.

Term	Definition
COS	The COS (802.1p) value for this rule.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The interface to which packets matching this rule are copied.
Redirect Interface	The interface to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the MAC ACL rule has referenced a time range.
Rule Status	Status (Active/Inactive) of the MAC ACL rule.
ACL Hit Count	The number of packets that match a configured ACL rule within an ACL (referred to as ACL hit count). The counter resets to 0 when the maximum value is reached. A dedicated counter exists for each ACL rule. ACL counters do not interact with PBR counters. For an ACL with multiple rules, if a match occurs for a specific rule, the counter that is associated with this rule increments. For example, if an ACL includes three rules, when a match occurs for rule 2, the counter for rule 3 does not increment. For ACL counters, if an ACL rule is configured without a rate limit condition, the counter shows the number of forwarded or discarded packets. (For example, for a burst of 100 packets, the counter shows 100.) If the ACL rule is configured with a rate limit condition, the counter shows the number of packets that match the condition: • If the packets are sent at a rate that is lower than the configured rate limit, the counter displays the number of packets that match the condition. • If the packets are sent at a rate that exceeds the configured rate limit, the counter still displays the number of packets that match the condition, even though packets are dropped beyond the configured limit. In this situation, the number of packets that match the condition equals the rate at which the packets are sent. For example, if the rate limit condition is 10 kbps but the matching traffic is sent at 100 kbps, the counter increments with 100 kbps. Either way, only the number of packets that match the condition is reflected in the counter, irrespective of whether they are dropped or forwarded. ACL counters do not interact with diffserv policies.

```
(NETGEAR Switch) #show mac access-lists mac1
```

```
ACL Name: mac1
```

```
Outbound Interface(s): control-plane
```

```
Sequence Number: 10
```

```
Action.....permit
```

```
Source MAC Address..... 00:00:00:00:AA:BB
```

```
Source MAC Mask.....FF:FF:FF:FF:00:00
```

```
Committed Rate.....32
```

```
Committed Burst Size.....16
```

```
ACL hit count .....0
```

```
Sequence Number: 25
```

```

Action.....permit
Source MAC Address.....00:00:00:00:AA:BB
Source MAC Mask.....FF:FF:FF:FF:00:00
Destination MAC Address.....01:80:C2:00:00:00
Destination MAC Mask.....00:00:00:FF:FF:FF
Ethertype.....ipv6
VLAN.....36
CoS Value.....7
Assign Queue.....4
Redirect Interface.....0/34
Committed Rate.....32
Committed Burst Size.....16
ACL hit count .....0

```

IP Access Control List Commands

This section describes the commands you use to configure IP Access Control List (ACL) settings. IP ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IP ACLs:

- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The maximum number of rules per IP ACL is hardware dependent.
- If you configure a MAC ACL on an interface, you cannot configure an IP ACL on the same interface.
- Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A 1 in a bit position of the ACL mask indicates the corresponding bit can be ignored.

access-list

M4250

M4350

This command creates an IP Access Control List (ACL) that is identified by the access list number, which is 1-99 for standard ACLs or 100-199 for extended ACLs. The table with parameters and descriptions on page [1324](#) describes the parameters for the **access-list** command.

The **sflow-remote-agent** option is supported on the M4350 series switch only.

IP Standard ACL:

Format	<code>access-list 1-99 [{remark comment [sequence-number]]} {deny permit} {every srcip srcmask host srcip} [time-range time-range-name] [log] [assign-queue queue-id] [{mirror redirect} {unit/slot/port lag lag-group-id}] [rate-limit rate burst-size] [slow-remote-agent]</code>

Mode	Global Config

IP Extended ACL:

Format	<code>access-list 100-199 [{remark comment [sequence-number]]} {deny permit} {every {{eigrp gre icmp igmp ip ipinip ospf pim tcp udp 0-255} {srcip srcmask any host srcip} [range {portkey startport} {portkey endport} {eq neq lt gt} {portkey 0-65535} {dstip dstmask any host dstip} [{range {portkey startport} {portkey endport} {eq neq lt gt} {portkey 0-65535}}] [flag [+fin -fin] [+syn -syn] [+rst -rst] [+psh -psh] [+ack -ack] [+urg -urg] [established]] [icmp-type icmp-type [icmp-code icmp-code] icmp-message icmp-message] [igmp-type igmp-type] [fragments] [precedence precedence tos tos [tosmask] dscp dscp] [ttl eq 0-255]]} [time-range time-range-name] [log] [assign-queue queue-id] [{mirror redirect} {unit/slot/port lag lag-group-id}] [rate-limit rate burst-size] [slow-remote-agent]</code>

Mode	Global Config

IPv4 extended ACLs have the following limitations for egress ACLs:

- Match on port ranges is not supported.
- The rate-limit command is not supported.

Note: An implicit **deny** all IP rule always terminates the access list.

Note: The **mirror** parameter allows the traffic matching this rule to be copied to the specified interface, while the **redirect** parameter allows the traffic matching this rule to be forwarded to the specified interface. The **assign-queue** and **redirect** parameters are only valid for a **permit** rule.

The **time-range** parameter allows imposing time limitation on the IP ACL rule as defined by the specified time range. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see [Time Range Commands for Time-Based ACLs on page 1349](#).

The **assign-queue** parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed *queue-id* value is 0-(*n*-1), in which *n* is the number of user configurable queues available for the hardware platform:

- M4250 series switch: from 0 to 7.
- M4350 series switch: from 0 to 6.

The **assign-queue** parameter is valid only for a **permit** rule.

The **permit** command's optional attribute **rate-limit** allows you to permit only the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

The **sflow-remote-agent** option is supported on the M4350 series switch only.

Parameter	Description
<i>1-99 or 100-199</i>	Range 1 to 99 is the access list number for an IP standard ACL. Range 100 to 199 is the access list number for an IP extended ACL.
<i>remark comment</i>	Use the remark keyword and <i>comment</i> parameter to add a comment (remark) to an IP standard or IP extended ACL. The remarks make the ACL easier to understand and scan. Each remark is limited to 100 characters. A remark can consist of characters in the range A–Z, a–z, and 0–9, and of special characters: space, hyphen, underscore. Remarks are displayed only in the output of the show running configuration command. For each IP standard or IP extended ACL rule, you can add one remark. You can remove only remarks that are not associated with a rule. Remarks that are associated with a rule are removed when the rule is removed.
<i>sequence-number</i>	The <i>sequence-number</i> parameter specifies the sequence number for the ACL rule. Either you define the sequence number or it is generated. If no sequence number exists for a rule, a sequence number that is 10 greater than the last sequence number in the ACL is used and the rule is placed at the end of the list. If this is the first ACL rule in the ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the creation of the ACL rule fails. You cannot create a rule that duplicates an already existing one and you cannot configure a rule with a sequence number that is already used for another rule. For example, if you add new ACL rule to the ACL without specifying a sequence number, the rule is placed at the bottom of the list. By changing the sequence number, you can move the ACL rule to a different position in the ACL.
<i>{deny permit}</i>	Specifies whether the IP ACL rule permits or denies an action. Note: For 5630x and 5650x-based systems, assign-queue, redirect, and mirror attributes are configurable for a deny rule, but they have no operational effect.
<i>every</i>	Match every packet.
<i>{eigrp gre icmp igmp ip ipinip ospf pim tcp udp 0-255}</i>	Specifies the protocol to filter for an extended IP ACL rule.

Parameter	Description
<code>srcip srcmask any host srcip</code>	Specifies a source IP address and source netmask for match condition of the IP ACL rule. Specifying any specifies <code>srcip</code> as 0.0.0.0 and <code>srcmask</code> as 255.255.255.255. Specifying host A.B.C.D specifies <code>srcip</code> as A.B.C.D and <code>srcmask</code> as 0.0.0.0.
<code>[{range {portkey startport} {portkey endport} {eq neq lt gt} {portkey 0-65535}]</code>	Note: This option is available only if the protocol is TCP or UDP. Specifies the source layer 4 port match condition for the IP ACL rule. You can use the port number, which ranges from 0-65535, or you specify the <code>portkey</code>, which can be one of the following keywords: - For TCP: bgp, domain, echo, ftp, ftp-data, http, smtp, telnet, www, pop2, or pop3. - For UDP: domain, echo, ntp, rip, snmp, tftp, time, or who. For both TCP and UDP, each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range. If range is specified, the IP ACL rule matches only if the layer 4 port number falls within the specified portrange. The <code>startport</code> and <code>endport</code> parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between will be part of the layer 4 port range. When eq is specified, the IP ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey. When lt is specified, IP ACL rule matches if the layer 4 port number is less than the specified port number or portkey. It is equivalent to specifying the range as 0 to <specified port number - 1>. When gt is specified, the IP ACL rule matches if the layer 4 port number is greater than the specified port number or portkey. It is equivalent to specifying the range as <specified port number + 1> to 65535. When neq is specified, IP ACL rule matches only if the layer 4 port number is not equal to the specified port number or portkey. Two rules are added in the hardware one with range equal to 0 to <specified port number - 1> and one with range equal to <specified port number + 1 to 65535>. Note: Port number matches only apply to unfragmented or first fragments.
<code>dstip dstmask any host dstip</code>	Specifies a destination IP address and netmask for match condition of the IP ACL rule. Specifying any implies specifying <code>dstip</code> as 0.0.0.0 and <code>dstmask</code> as 255.255.255.255. Specifying host A.B.C.D implies <code>dstip</code> as A.B.C.D and <code>dstmask</code> as 0.0.0.0.
<code>[precedence precedence tos tos [tosmask] dscp dscp]</code>	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters <code>precedence</code>, <code>tos</code> or <code>dscp</code>. <code>tosmask</code> is an optional parameter.

Parameter	Description
<code>flag [+fin -fin] [+syn -syn] [+rst -rst] [+psh -psh] [+ack -ack] [+urg -urg] [established]</code>	Note: This option is available only if the protocol is <code>tcp</code>. Specifies that the IP ACL rule matches on the TCP flags. When <code>+<tcpflagname></code> is specified, a match occurs if the specified <code><tcpflagname></code> flag is set in the TCP header. When <code>-<tcpflagname></code> is specified, a match occurs if the specified <code><tcpflagname></code> flag is not set in the TCP header. When <code>established</code> is specified, a match occurs if the specified RST or ACK bits are set in the TCP header. Two rules are installed in the hardware when the <code>established</code> option is specified.
<code>[icmp-type <i>icmp-type</i> [icmp-code <i>icmp-code</i>] icmp-message <i>icmp-message</i>]</code>	Note: This option is available only if the protocol is <code>icmp</code>. Specifies a match condition for ICMP packets. When <code>icmp-type</code> is specified, the IP ACL rule matches on the specified ICMP message type, a number from 0 to 255. When <code>icmp-code</code> is specified, the IP ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying <code>icmp-message</code> implies that both <code>icmp-type</code> and <code>icmp-code</code> are specified. The following <code>icmp-message</code> options are supported: 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.
<code>igmp-type <i>igmp-type</i></code>	This option is available only if the protocol is <code>igmp</code>. When <code>igmp-type</code> is specified, the IP ACL rule matches on the specified IGMP message type, a number from 0 to 255.
<code>[ttl eq 0-255]</code>	Specifies that the TTL value in the packet must be equal to the TTL value, which can be from 0 to 255.
<code>fragments</code>	Specifies that the IP ACL rule matches on fragmented IP packets.
<code>[log]</code>	Specifies that this rule is to be logged.
<code>[time-range <i>time-range-name</i>]</code>	Allows imposing time limitation on the ACL rule as defined by the parameter <code>time-range-name</code>. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see Time Range Commands for Time-Based ACLs on page 1349.
<code>[assign-queue <i>queue-id</i>]</code>	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned: • M4250 series switch: from 0 to 7. • M4350 series switch: from 0 to 6.

Parameter	Description
<code>[{mirror redirect} {unit/slot/port lag lag-group-id}]</code>	Specifies the mirror or redirect interface or <i>lag-group-id</i> to which packets matching this rule are copied or forwarded. To specify an actual interface or port, do the following: - For an M4250 series switch, use the argument <i>slot/port</i>. - For an M4350 series switch, use the argument <i>unit/slot/port</i>, as shown in the command format.
<code>[rate-limit rate burst-size]</code>	Specifies the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.
<code>[sflow-remote-agent]</code>	This option is supported on the M4350 series switch only. Specifies that sFlow sampling must occur, allowing packets that are matching the rule to be copied to the remote sFlow agent.

no access-list

This command deletes an IP ACL that is identified by the parameter *accesslistnumber* from the system. The range for *accesslistnumber* is 1–99 for standard access lists and 100–199 for extended access lists.

Format	<code>no access-list accesslistnumber</code>

Mode	Global Config

ip access-list

M4250

M4350

This command creates an extended IP Access Control List (ACL) identified by name, consisting of classification fields defined for the IP header of an IPv4 frame. The *name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list. The rate-limit attribute configures the committed rate and the committed burst size.

If an IP ACL by this name already exists, this command enters IPv4-Access_List config mode to allow updating the existing IP ACL.

Note: The CLI mode changes to IPv4-Access-List Config mode when you successfully execute this command.

Format	<code>ip access-list name</code>

Mode	Global Config

no ip access-list

This command deletes the IP ACL identified by name from the system.

Format	no ip access-list <i>name</i>
Mode	Global Config

ip access-list resequence

M4250

M4350

Use this command to renumber the sequence of the entries for a specified IP access list with a specified increment value, starting from a specified sequence number. That is, with this command you can change the sequence numbers of ACL rules in the ACL and, therefore, change the order in which entries are applied. This command is not saved in the startup configuration and does not display in the running configuration.

Note: If the generated sequence number exceeds the maximum sequence number, the ACL rule creation fails and an informational message displays.

Default	10
Format	ip access-list resequence { <i>name</i> <i>id</i> } <i>starting-sequence-number</i> <i>increment</i>
Mode	Global Config
Parameter	Description
name	The name of the access control list.
id	The ID of the access control list.
starting-sequence-number	The sequence number from which to start the renumbering. The range is 1–2147483647. The default is 10.
increment	The value with which the sequence numbers must be incremented. The range is 1–2147483647. The default is 10.

ip access-list rename

M4250

M4350

This command changes the name of an IP Access Control List (ACL). The *name* parameter is the names of an existing IP ACL. The *newname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

This command fails if an IP ACL by the name that is defined by *newname* already exists.

Format	<code>ip access-list rename <i>name newname</i></code>

Mode	Global Config

[sequence-number] {deny | permit} (IP ACL)

M4250

M4350

This command creates a new rule for the current IP access list. Each rule is appended to the list of configured rules for the list. A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the every keyword or the protocol, source address, and destination address values must be specified. The source and destination IP address fields may be specified using the keyword **any** to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

Format	<code>[sequence-number] {deny permit} {every {{eigrp gre icmp igmp ip ipinip ospf pim tcp udp 0-255} {srcip srcmask any host srcip} [{range {portkey startport} {portkey endport} {eq neq lt gt} {portkey 0-65535}}] {dstip dstmask any host dstip} [{range {portkey startport} {portkey endport} {eq neq lt gt} {portkey 0-65535}}] [flag [+fin -fin] [+syn -syn] [+rst -rst] [+psh -psh] [+ack -ack] [+urg -urg] [established]] [icmp-type icmp-type [icmp-code icmp-code] icmp-message icmp-message] [igmp-type igmp-type] [fragments] [precedence precedence tos tos [tosmask] dscp dscp] [ttl eq 0-255]]} [time-range time-range-name] [log] [assign-queue queue-id] [{mirror redirect} {unit/slot/port lag lag-group-id}] [rate-limit rate burst-size] [slow-remote-agent]</code>

Mode	Ipv4-Access-List Config

Note: An implicit **deny** all IP rule always terminates the access list.

Note: The **mirror** parameter allows the traffic matching this rule to be copied to the specified interface, while the **redirect** parameter allows the traffic matching this rule to be forwarded to the specified interface. The **assign-queue** and **redirect** parameters are only valid for a **permit** rule.

For IPv4, the following are not supported for egress ACLs:

- A match on port ranges.
- The rate-limit command.

The **time-range** parameter allows imposing time limitation on the IP ACL rule as defined by the specified time range. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see [Time Range Commands for Time-Based ACLs on page 1349](#).

The **assign-queue** parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed *queue-id* value is 0-(*n*-1), in which *n* is the number of user configurable queues available for the hardware platform:

- M4250 series switch: from 0 to 7.
- M4350 series switch: from 0 to 6.

The **assign-queue** parameter is valid only for a **permit** rule.

The **permit** command's optional attribute **rate-limit** allows you to permit only the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

The **sflow-remote-agent** option is supported on the M4350 series switch only.

Table 13. IP ACL command parameters

Parameter	Description
<i>sequence-number</i>	The <i>sequence-number</i> parameter specifies the sequence number for the ACL rule. Either you define the sequence number or is it is generated. If no sequence number exists for a rule, a sequence that is 10 greater than the last sequence number in the ACL is used and the rule is placed at the end of the list. If this is the first ACL rule in the ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the creation of the ACL rule fails. You cannot create a rule that duplicates an already existing one and you cannot configure a rule with a sequence number that is already used for another rule. For example, if you add new ACL rule to the ACL without specifying a sequence number, the rule is placed at the bottom of the list. By changing the sequence number, you can move the ACL rule to a different position in the ACL.
{deny permit}	Specifies whether the IP ACL rule permits or denies the matching traffic.
every	Match every packet.
{eigrp gre icmp igmp ip ipinip ospf pim tcp udp 0-255}	Specifies the protocol to match for the IP ACL rule.

Table 13. IP ACL command parameters (continued)

Parameter	Description
<code>srcip srcmask any host srcip</code>	Specifies a source IP address and source netmask to match for the IP ACL rule. Specifying “any” implies specifying <code>srcip</code> as “0.0.0.0” and <code>srcmask</code> as “255.255.255.255”. Specifying “host A.B.C.D” implies <code>srcip</code> as “A.B.C.D” and <code>srcmask</code> as “0.0.0.0”.
<code>[{range {portkey startport} {portkey endport} {eq neq lt gt} {portkey 0-65535}]</code>	Note: This option is available only if the protocol is <code>tcp</code> or <code>udp</code>. Specifies the layer 4 port match condition for the IP ACL rule. Port number can be used, which ranges from 0-65535, or the portkey, which can be one of the following keywords: For tcp protocol: <code>bgp</code>, <code>domain</code>, <code>echo</code>, <code>ftp</code>, <code>ftp-data</code>, <code>http</code>, <code>smtp</code>, <code>telnet</code>, <code>www</code>, <code>pop2</code>, or <code>pop3</code>. For udp protocol: <code>domain</code>, <code>echo</code>, <code>ntp</code>, <code>rip</code>, <code>snmp</code>, <code>tftp</code>, <code>time</code>, or <code>who</code>. Each of these keywords translates into its equivalent port number. When range is specified, the IP ACL rule matches only if the layer 4 port number falls within the specified port range. The <code>startport</code> and <code>endport</code> parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal to or greater than the starting port. The starting port, ending port, and all ports in between will be part of the layer 4 port range. When eq is specified, IP ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey. When lt is specified, IP ACL rule matches if the layer 4 port number is less than the specified port number or portkey. It is equivalent to specifying the range as 0 to <specified port number - 1>. When gt is specified, IP ACL rule matches if the layer 4 port number is greater than the specified port number or portkey. It is equivalent to specifying the range as <specified port number + 1> to 65535. When neq is specified, IP ACL rule matches only if the layer 4 port number is not equal to the specified port number or port key. Two rules are added in the hardware one with range equal to 0 to <specified port number - 1> and one with range equal to <specified port number + 1 to 65535>. Note: Port number matches only apply to unfragmented or first fragments.
<code>dstip dstmask any host dstip</code>	Specifies a destination IP address and netmask for match condition of the IP ACL rule. Specifying any implies specifying <code>dstip</code> as 0.0.0.0 and <code>dstmask</code> as 255.255.255.255. Specifying host A.B.C.D implies <code>dstip</code> as A.B.C.D and <code>dstmask</code> as 0.0.0.0.

Table 13. IP ACL command parameters (continued)

Parameter	Description
<code>[precedence <i>precedence</i> tos <i>tos</i> [tosmask] dscp <i>dscp</i>]</code>	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters <i>precedence</i> , <i>tos</i> or <i>dscp</i> . <i>tosmask</i> is an optional parameter.
<code>flag [+fin -fin] [+syn -syn] [+rst -rst] [+psh -psh] [+ack -ack] [+urg -urg] [established]</code>	Specifies that the IP ACL rule matches on the tcp flags. When +<tcpflagname> is specified, a match occurs if specified <tcpflagname> flag is set in the TCP header. When -<tcpflagname> is specified, a match occurs if specified <tcpflagname> flag is NOT set in the TCP header. When established is specified, a match occurs if either the specified RST or ACK bits are set in the TCP header. Two rules are installed in hardware to when the established option is specified. This option is available only if protocol is tcp.
<code>[icmp-type <i>icmp-type</i> [icmp-code <i>icmp-code</i> icmp-message <i>icmp-message</i>]</code>	Note: This option is available only if the protocol is ICMP. Specifies a match condition for ICMP packets. When icmp-type is specified, IP ACL rule matches on the specified ICMP message type, a number from 0 to 255. When icmp-code is specified, IP ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying icmp-message implies both <i>icmp-type</i> and <i>icmp-code</i> are specified. The following <i>icmp-message</i> options are supported: 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. The ICMP message is decoded into corresponding ICMP type and ICMP code within that ICMP type.
<code>igmp-type <i>igmp-type</i></code>	Note: This option is visible only if the protocol is IGMP. When igmp-type is specified, the IP ACL rule matches on the specified IGMP message type, a number from 0 to 255.
<code>[ttl eq 0-255]</code>	Specifies that the TTL value in the packet must be equal to the TTL value, which can be from 0 to 255.
<code>fragments</code>	Specifies that the IP ACL rule matches on noninitial fragmented packets where the fragment extension header contains a nonzero fragment offset. The fragments keyword is an option only if the protocol is ipv6 and the operator port-number arguments are not specified.
<code>log</code>	Specifies that this rule is to be logged.

Table 13. IP ACL command parameters (continued)

Parameter	Description
<code>time-range <i>time-range-name</i></code>	Allows imposing a time limitation on the ACL rule as defined by the parameter <i>time-range-name</i> . If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.
<code>[assign-queue <i>queue-id</i>]</code>	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned: • M4250 series switch: from 0 to 7. • M4350 series switch: from 0 to 6.
<code>[{mirror redirect} {<i>unit/slot/port</i> lag <i>lag-group-id</i>}]</code>	Specifies the mirror or redirect interface or <i>lag-group-id</i> to which packets matching this rule are copied or forwarded. To specify an actual interface or port, do the following: • For an M4250 series switch, use the argument <i>slot/port</i>. • For an M4350 series switch, use the argument <i>unit/slot/port</i>, as shown in the command format.
<code>rate-limit <i>rate burst-size</i></code>	Specifies the allowed rate of traffic as per the configured <i>rate</i> in kbps, and <i>burst-size</i> in kbytes.
<code>[sflow-remote-agent]</code>	This option is supported on the M4350 series switch only. Specifies that sFlow sampling must occur, allowing packets that are matching the rule to be copied to the remote sFlow agent.

Command example:

```
(NETGEAR Switch) (Config)#ip access-list ip1
```

```
(NETGEAR Switch) (Config-ipv4-acl)#permit icmp any any rate-limit 32 16
```

```
(NETGEAR Switch) (Config-ipv4-acl)#exit
```

no sequence-number (IP ACL)

Use this command to remove the ACL rule with the specified sequence number from the ACL.

Format	<code>no sequence-number</code>
Modes	Ipv4-Access-List Config

ip access-group

M4250**M4350**

This command either attaches a specific IP Access Control List (ACL) identified by *acl-number* or *name* to an interface, range of interfaces, or all interfaces; or associates it with a VLAN ID in a specific direction. The parameter *name* is the name of the Access Control List.

An optional sequence number may be specified to indicate the order of this IP access list relative to other IP access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached IP access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

An optional *control-plane* is specified to apply the ACL on CPU port. The IPv4 control packets like RADIUS and TACACS+ are also dropped because of the implicit **deny all** rule added at the end of the list. To overcome this, permit rules must be added to allow the IPv4 control packets.

Note: The **control-plane** keyword is available only in Global Config mode.
Depending on the platform, the **out** option might not be available.

Default	none
Format	ip access-group { <i>acl-number</i> <i>name</i> } [{control-plane in out} vlan <i>vlan-id</i> {in out}] [sequence 1-4294967295]
Modes	Interface Config Global Config

Parameter	Description
<i>acl-number</i>	Identifies a specific IP ACL. The range is 1 to 199.
<i>name</i>	The name of the Access Control List.
<i>vlan-id</i>	A VLAN ID associated with a specific IP ACL.
<i>sequence</i>	A optional sequence number that indicates the order of this IP access list relative to the other IP access lists already assigned to this interface and direction. The range is 1 to 4294967295.

```
(NETGEAR Switch) (Config)#ip access-group ipl control-plane
```

no ip access-group

This command removes a specified IP ACL from an interface.

Default	none
Format	no ip access-group { <i>acl-number</i> <i>name</i> } [{control-plane in out}] vlan <i>vlan-id</i> {in out}}
Mode	Interface Config Global Config

Command example:

```
(NETGEAR Switch) (Config) #no ip access-group ip1 control-plane
```

acl-trapflags

M4250

M4350

This command enables the ACL trap mode.

Default	disabled
Format	acl-trapflags
Mode	Global Config

no acl-trapflags

This command disables the ACL trap mode.

Format	no acl-trapflags
Mode	Global Config

show ip access-lists

M4250

M4350

Use this command to view summary information about all IP ACLs that are configured on the switch. To view more detailed information about a specific access list, specify the ACL number or name that is used to identify the IP ACL. The command output displays the committed rate, committed burst size, and the number of packets that match a configured ACL rule within an ACL (referred to as ACL hit count).

Format	show ip access-lists [<i>acl-number</i> <i>name</i>]
Mode	Privileged EXEC

Term	Definition
ACL ID/Name	Identifies the configured ACL number or name.
Rules	Identifies the number of rules configured for the ACL.
Direction	Shows whether the ACL is applied to traffic coming into the interface (ingress) or leaving the interface (egress).
Interface(s)	Identifies the interface(s) to which the ACL is applied (ACL interface bindings).
VLAN(s)	Identifies the VLANs to which the ACL is applied (ACL VLAN bindings).

If you specify an IP ACL number or name, the following information displays:

Note: Only the access list fields that you configure are displayed. Thus, the command output varies based on the match criteria configured within the rules of an ACL.

Term	Definition
Rule Number	The number identifier for each rule that is defined for the IP ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	The protocol to filter for this rule.
ICMP Type	Note: This is shown only if the protocol is ICMP. The ICMP message type for this rule.
Starting Source L4 port	The starting source layer 4 port.
Ending Source L4 port	The ending source layer 4 port.
Starting Destination L4 port	The starting destination layer 4 port.
Ending Destination L4 port	The ending destination layer 4 port.
ICMP Code	Note: This is shown only if the protocol is ICMP. The ICMP message code for this rule.
Fragments	If the ACL rule matches on fragmented IP packets.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Source IP Address	The source IP address for this rule.
Source IP Mask	The source IP Mask for this rule.
Source L4 Port Keyword	The source port for this rule.

Term	Definition
Destination IP Address	The destination IP address for this rule.
Destination IP Mask	The destination IP Mask for this rule.
Destination L4 Port Keyword	The destination port for this rule.
IP DSCP	The value specified for IP DSCP.
IP Precedence	The value specified IP Precedence.
IP TOS	The value specified for IP TOS.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The unit/port to which packets matching this rule are copied.
Redirect Interface	The unit/port to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the IP ACL rule has referenced a time range.
Rule Status	Status (Active/Inactive) of the IP ACL rule.
ACL Hit Count	The number of packets that match a configured ACL rule within an ACL (referred to as ACL hit count). The counter resets to 0 when the maximum value is reached. A dedicated counter exists for each ACL rule. ACL counters do not interact with PBR counters. For an ACL with multiple rules, if a match occurs for a specific rule, the counter that is associated with this rule increments. For example, if an ACL includes three rules, when a match occurs for rule 2, the counter for rule 3 does not increment. For ACL counters, if an ACL rule is configured without a rate limit condition, the counter shows the number of forwarded and or discarded packets. (For example, for a burst of 100 packets, the counter shows 100.) If the ACL rule is configured with a rate limit condition, the counter shows the number of packets that match the condition: • If the packets are sent at a rate that is lower than the configured rate limit, the counter displays the number of packets that match the condition. • If the packets are sent at a rate that exceeds the configured rate limit, the counter still displays the number of packets that match the condition, even though packets are dropped beyond the configured limit. In this situation, the number of packets that match the condition equals the rate at which the packets are sent. For example, if the rate limit condition is 10 kbps but the matching traffic is sent at 100 kbps, the counter increments with 100 kbps. Either way, only the number of packets that match the condition is reflected in the counter, irrespective of whether they are dropped or forwarded. ACL counters do not interact with diffserv policies.

Command example:

```
(NETGEAR Switch) #show ip access-lists ip1
```

```
ACL Name: ip1
```

```
Inbound Interface(s): 1/0/30
```

```

Rule Number: 1
Action..... permit
Match All..... FALSE
Protocol..... 1 icmp
Committed Rate..... 32
Committed Burst Size..... 16
ACL hit count .....0

```

show access-lists interface

M4250

M4350

This command displays IP ACLs, IPv6 ACLs, and MAC access control lists information for a designated interface and direction (in or out). To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Use **lag** *lag-intf-num* to specify the LAG interface, in which *lag-intf-num* is the LAG port number.

Use the **control-plane** keyword to display the ACLs applied on the CPU port.

Format `show access-lists interface {unit/slot/port | lag lag-int-num} {in | out | control-plane}`

Mode Privileged EXEC

Term	Definition
ACL Type	Type of access list (IP, IPv6, or MAC).
ACL ID	Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.
Sequence Number	A sequence number indicates the order of the access list relative to other access lists already assigned to this interface and direction.
in or out	• in – Display Access List information for a particular interface and the in direction. • out – Display Access List information for a particular interface and the out direction.

Command example:

```
(NETGEAR Switch) #show access-lists interface control-plane
```

ACL Type	ACL ID	Sequence Number
-----	-----	-----
IPv6	ip61	1

show access-lists vlan

M4250

M4350

This command displays access list information for a particular VLAN ID. The *vlan-id* parameter is the VLAN ID of the VLAN with the information to view. The **in** and **out** options specify the direction of the VLAN ACL information to view.

Format	show access-lists vlan <i>vlan-id</i> [in out]
Mode	Privileged EXEC
Term	Definition
ACL Type	Type of access list (IP, IPv6, or MAC).
ACL ID	Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.
Sequence Number	A sequence number indicates the order of the access list relative to other access lists already assigned to this interface and direction.
in or out	- in – Display Access List information for a particular interface and the in direction. - out – Display Access List information for a particular interface and the out direction.

IPv6 Access Control List Commands

This section describes the commands you use to configure IPv6 Access Control List (ACL) settings. IPv6 ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IPv6 ACLs:

- The maximum number of ACLs you create is 100, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per IPv6 ACL is hardware dependent.

ipv6 access-list

M4250

M4350

This command creates an IPv6 Access Control List (ACL) identified by name, consisting of classification fields defined for the IP header of an IPv6 frame. The *name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list. The rate-limit attribute configures the committed rate and the committed burst size.

If an IPv6 ACL by this name already exists, this command enters IPv6-Access-List config mode to allow updating the existing IPv6 ACL.

Note: The CLI mode changes to IPv6-Access-List Config mode when you successfully execute this command.

Format	<code>ipv6 access-list <i>name</i></code>

Mode	Global Config

`no ipv6 access-list`

This command deletes the IPv6 ACL identified by *name* from the system.

Format	<code>no ipv6 access-list <i>name</i></code>

Mode	Global Config

`ipv6 access-list rename`

M4250

M4350

This command changes the name of an IPv6 ACL. The *name* parameter is the name of an existing IPv6 ACL. The *newname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

This command fails if an IPv6 ACL by the name that is specified by the *newname* argument already exists.

Format	<code>ipv6 access-list rename <i>name newname</i></code>

Mode	Global Config

`ipv6 access-list resequence`

M4250

M4350

Use this command to renumber the sequence of the entries for a specified IPv6 access list with a specified increment value, starting from a specified sequence number. That is, with this command you can change the sequence numbers of ACL rules in the ACL and, therefore, change the order in which entries are applied. This command is not saved in the startup configuration and does not display in the running configuration.

Note: If the generated sequence number exceeds the maximum sequence number, the ACL rule creation fails and an informational message displays.

Default	10
Format	<code>ipv6 access-list resequence name starting-sequence-number increment</code>
Mode	Global Config

Parameter	Description
name	The name of the access control list.
id	The ID of the access control list.
starting-sequence-number	The sequence number from which to start the renumbering. The range is 1–2147483647. The default is 10.
increment	The value with which the sequence numbers must be incremented. The range is 1–2147483647. The default is 10.

{deny | permit} (IPv6 ACL)

M4250

M4350

This command creates a new rule for the current IPv6 access list. Each rule is appended to the list of configured rules for the list. A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the **every** keyword or the protocol, source address, and destination address values must be specified. The source and destination IPv6 address fields may be specified using the keyword **any** to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

Format	<code>{deny permit} {every {{icmpv6 ipv6 tcp udp 0-255} {source-ipv6-prefix/prefix-length any host source-ipv6-address} [eq {portkey 0-65535}] {destination-ipv6-prefix/prefix-length any host destination-ipv6-address} [eq {portkey 0-65535}] [flag [+fin -fin] [+syn -syn] [+rst -rst] [+psh -psh] [+ack -ack] [+urg -urg] [established]] [flow-label value] [icmp-type icmp-type [icmp-code icmp-code] icmp-message icmp-message] [fragments] [sequence sequence-number] [dscp dscp] [ttl eq 0-255]]} [log] [assign-queue queue-id] [{mirror redirect} unit/port] [rate-limit rate burst-size] [slow-remote-agent]</code>
Mode	IPv6-Access-List Config

Note: An implicit **deny all IPv6** rule always terminates the access list.

The **time-range** parameter allows imposing time limitation on the IPv6 ACL rule as defined by the parameter *time-range-name*. If a time range with the specified name does not exist

and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see [Time Range Commands for Time-Based ACLs on page 1349](#).

The **assign-queue** parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed *queue-id* value is 0-(*n*-1), in which *n* is the number of user configurable queues available for the hardware platform:

- M4250 series switch: from 0 to 7.
- M4350 series switch: from 0 to 6.

The **assign-queue** parameter is valid only for a permit rule.

Note: The **mirror** parameter allows the traffic matching this rule to be copied to the specified interface, while the **redirect** parameter allows the traffic matching this rule to be forwarded to the specified interface. The **assign-queue** and **redirect** parameters are only valid for a **permit** rule.

The **permit** command's optional attribute **rate-limit** allows you to permit only the allowed rate of traffic as per the configured *rate* in kbps, and *burst-size* in kbytes.

IPv6 ACLs have the following limitations:

- Port ranges are not supported for egress IPv6 ACLs.
- The rate-limit command is not supported for egress IPv6 ACLs.

The **sflow-remote-agent** option is supported on the M4350 series switch only.

Table 14. IPv6 ACL command parameters

Parameter	Description
{deny permit}	Specifies whether the IPv6 ACL rule permits or denies the matching traffic.
every	Specifies to match every packet.
{protocolkey number}	Specifies the protocol to match for the IPv6 ACL rule. The current list is: icmpv6 , ipv6 , tcp , and udp .

Table 14. IPv6 ACL command parameters (continued)

Parameter	Description
<i>source-ipv6-prefix/prefix-length</i> <i>any</i> <i>host source-ipv6-address</i>	For <i>source-ipv6-prefix/prefix-length</i>, specify a source IPv6 source address and prefix length to match for the IPv6 ACL rule. Specifying any implies specifying <code>::/0</code> Specifying <i>host source-ipv6-address</i> implies matching the specified IPv6 address. The <i>source-ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
[<i>eq {portkey 0-65535}</i>]	Note: This option is available only if the protocol is TCP or UDP. Specifies the layer 4 port match condition for the IPv6 ACL rule. A port number can be used, in the range 0-65535, or the <i>portkey</i>, which can be one of the following keywords: For TCP: bgp, domain, echo, ftp, ftp-data, http, smtp, telnet, www, pop2, or pop3. For UDP: domain, echo, ntp, rip, snmp, tftp, time, or who. Each of these keywords translates into its equivalent port number. When eq is specified, the IPv6 ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey. Two rules are added in the hardware one with range equal to 0 to <specified port number - 1> and one with range equal to <specified port number + 1 to 65535>
<i>destination-ipv6-prefix/prefix-length</i> <i>any</i> <i>host destination-ipv6-address</i>	For <i>destination-ipv6-prefix/prefix-length</i>, specify a destination IPv6 source address and prefix length to match for the IPv6 ACL rule. Specifying any implies specifying <code>::/0</code> Specifying <i>host destination-ipv6-address</i> implies matching the specified IPv6 address. This <i>destination-ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
[<i>dscp dscp</i>]	Specifies the <i>dscp</i> value to match for the IPv6 rule.
<i>flag</i> [+ <i>fin</i> - <i>fin</i>] [+ <i>syn</i> - <i>syn</i>] [+ <i>rst</i> - <i>rst</i>] [+ <i>psh</i> - <i>psh</i>] [+ <i>ack</i> - <i>ack</i>] [+ <i>urg</i> - <i>urg</i>] [<i>established</i>]	Specifies that the IPv6 ACL rule matches on the tcp flags. When +<tcpflagname> is specified, a match occurs if specified <tcpflagname> flag is set in the TCP header. When "-<tcpflagname>" is specified, a match occurs if specified <tcpflagname> flag is not set in the TCP header. When <i>established</i> is specified, a match occurs if specified either RST or ACK bits are set in the TCP header. Two rules are installed in hardware to when "established" option is specified. This option is visible only if protocol is tcp.

Table 14. IPv6 ACL command parameters (continued)

Parameter	Description
<code>[icmp-type <i>icmp-type</i> [icmp-code <i>icmp-code</i>] icmp-message <i>icmp-message</i>]</code>	Note: This option is available only if the protocol is icmpv6. Specifies a match condition for ICMP packets. When icmp-type is specified, IPv6 ACL rule matches on the specified ICMP message type, a number from 0 to 255. When icmp-code is specified, IPv6 ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying icmp-message implies both <i>icmp-type</i> and <i>icmp-code</i> are specified. The following <i>icmp-message</i> options are supported: 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. The ICMP message is decoded into the corresponding ICMP type and ICMP code within that ICMP type.
<code>[ttl eq <i>ttl-value</i>]</code>	Specifies that the TTL value in the packet must be equal to the TTL value specified in <i>.ttl-value</i> .
<code>fragments</code>	Specifies that IPv6 ACL rule matches on fragmented IPv6 packets (Packets that have the next header field is set to 44).
<code>log</code>	Specifies that this rule is to be logged.
<code>[time-range <i>time-range-name</i>]</code>	Allows imposing a time limitation on the ACL rule as defined by the parameter <i>time-range-name</i> . If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied immediately. If a time range with the specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied when the time-range with the specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.
<code>[assign-queue <i>queue-id</i>]</code>	Specifies the assign-queue, which is the queue identifier (<i>queue-id</i>) to which packets matching this rule are assigned: • M4250 series switch: from 0 to 7. • M4350 series switch: from 0 to 6.
<code>[{mirror redirect} {unit/slot/port lag <i>lag-group-id</i>}]</code>	Specifies the mirror or redirect interface or <i>lag-group-id</i> to which packets matching this rule are copied or forwarded. To specify an actual interface or port, do the following: • For an M4250 series switch, use the argument <i>slot/port</i>. • For an M4350 series switch, use the argument <i>unit/slot/port</i>, as shown in the command format.

Table 14. IPv6 ACL command parameters (continued)

Parameter	Description
[rate-limit <i>rate burst-size</i>]	Specifies the allowed rate of traffic as per the configured <i>rate</i> in kbps, and <i>burst-size</i> in kbytes.
[sflow-remote-agent]	This option is supported on the M4350 series switch only. Specifies that sFlow sampling must occur, allowing packets that are matching the rule to be copied to the remote sFlow agent.

Command example:

```
(NETGEAR Switch) (Config)#ipv6 access-list ip61
(NETGEAR Switch) (Config-ipv6-acl)#permit udp any any rate-limit 32 16
(NETGEAR Switch) (Config-ipv6-acl)#exit
```

no sequence-number (IPv6 ACL)

Use this command to remove the ACL rule with the specified sequence number from the ACL.

Format	no <i>sequence-number</i>
Modes	IPv6-Access-List Config

ipv6 traffic-filter

M4250

M4350

This command either attaches a specific IPv6 ACL identified by name to an interface or range of interfaces, or associates it with a VLAN ID in a specific direction. The *name* parameter must be the name of an existing IPv6 ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other IPv6 access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified IPv6 access list replaces the currently attached IPv6 access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The **vlan** keyword and *vlan-id* argument are valid only in the Global Config mode. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

An optional *control-plane* is specified to apply the ACL on CPU port. The IPv6 control packets like IGMPv6 are also dropped because of the implicit **deny all** rule added at the end of the list. To overcome this, permit rules must be added to allow the IPv6 control packets.

Note: The **control-plane** keyword is available only in Global Config mode.

Depending on the platform, the **out** option might not be available.

Format	<code>ipv6 traffic-filter <i>name</i> {{control-plane in out} vlan <i>vlan-id</i> {in out}} [sequence 1-4294967295]</code>
Modes	Global Config Interface Config

```
(NETGEAR Switch) (Config)#ipv6 traffic-filter ip61 control-plane
```

no ipv6 traffic-filter

This command removes an IPv6 ACL identified by *name* from the interface(s) in a specified direction.

Format	<code>no ipv6 traffic-filter name {{control-plane in out} vlan <i>vlan-id</i> {in out}}</code>
Modes	Global Config Interface Config

Command example:

```
(NETGEAR Switch) (Config)#no ipv6 traffic-filter ip61 control-plane
```

show ipv6 access-lists

M4250

M4350

Use this command to view summary information about all IPv6 ACLs that are configured on the switch. To view more detailed information about a specific access list, specify the ACL name that is used to identify the IP ACL. The command output displays the ICMP type, ICMP code, fragments, routing, and TCP flags attributes, the source and destination L4 port ranges, and the number of packets that match a configured ACL rule within an ACL (referred to as ACL hit count).

Format	<code>show ipv6 access-lists [<i>name</i>]</code>
Mode	Privileged EXEC

Note: Only the access list fields that you configure are displayed. Therefore, the command output varies based on the match criteria configured within the rules of an ACL.

Term	Definition
Action	The action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	The protocol to filter for this rule.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Source IP Address	The source IP address for this rule.
Source L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination L4 Port Keyword	The destination port for this rule.
IP DSCP	The value specified for IP DSCP.
Flow Label	The value specified for IPv6 Flow Label.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The interface to which packets matching this rule are copied.
Redirect Interface	The interface to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the IPv6 ACL rule has referenced a time range.

Term	Definition
Rule Status	Status (Active/Inactive) of the IPv6 ACL rule.
ACL Hit Count	The number of packets that match a configured ACL rule within an ACL (referred to as ACL hit count). The counter resets to 0 when the maximum value is reached. A dedicated counter exists for each ACL rule. ACL counters do not interact with PBR counters. For an ACL with multiple rules, if a match occurs for a specific rule, the counter that is associated with this rule increments. For example, if an ACL includes three rules, when a match occurs for rule 2, the counter for rule 3 does not increment. For ACL counters, if an ACL rule is configured without a rate limit condition, the counter shows the number of forwarded or discarded packets. (For example, for a burst of 100 packets, the counter shows 100.) If the ACL rule is configured with a rate limit condition, the counter shows the number of packets that match the condition: • If the packets are sent at a rate that is lower than the configured rate limit, the counter displays the number of packets that match the condition. • If the packets are sent at a rate that exceeds the configured rate limit, the counter still displays the number of packets that match the condition, even though packets are dropped beyond the configured limit. In this situation, the number of packets that match the condition equals the rate at which the packets are sent. For example, if the rate limit condition is 10 kbps but the matching traffic is sent at 100 kbps, the counter increments with 100 kbps. Either way, only the number of packets that match the condition is reflected in the counter, irrespective of whether they are dropped or forwarded. ACL counters do not interact with diffserv policies.

Command example:

```
(NETGEAR Switch) #show ipv6 access-lists ip61
```

```
ACL Name: ip61
```

```
Outbound Interface(s): control-plane
```

```
Rule Number: 1
```

```
Action..... permit
Match Every..... FALSE
Protocol..... 17(udp)
Committed Rate..... 32
Committed Burst Size..... 16
ACL hit count .....0
```

Time Range Commands for Time-Based ACLs

Time-based ACLs allow one or more rules within an ACL to be based on time. Each ACL rule within an ACL except for the implicit **deny all** rule can be configured to be active and operational only during a specific time period. The time range commands allow you to define specific times of the day and week in order to implement time-based ACLs. The time range is identified by a name and can then be referenced by an ACL rule defined with in an ACL.

time-range

M4250

M4350

Use this command to create a time range identified by name, consisting of one absolute time entry and/or one or more periodic time entries. The *name* parameter is a case-sensitive, alphanumeric string from 1 to 31 characters that uniquely identifies the time range. An alpha-numeric string is defined as consisting of only alphabetic, numeric, dash, underscore, or space characters.

If a time range by this name already exists, this command enters Time-Range config mode to allow updating the time range entries

Note: When you successfully execute this command, the CLI mode changes to Time-Range Config mode.

Format	time-range <i>name</i>
Mode	Global Config

no time-range

This command deletes a time-range identified by *name*.

Format	no time-range <i>name</i>
Mode	Global Config

absolute

M4250

M4350

Use this command to add an absolute time entry to a time range. Only one absolute time entry is allowed per time-range. The *time* parameter is based on the currently configured time zone.

The optional **start** *time date* parameters indicate the time and date at which the configuration that referenced the time range starts going into effect. The time is expressed in a 24-hour clock, in the form of hours:minutes. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm. The date is expressed in the format day month year. If no start time and date are specified, the configuration statement is in effect immediately.

The optional **end** *time date* parameters indicate the time and date at which the configuration that referenced the time range is no longer in effect. The end time and date must be after the start time and date. If no end time and date are specified, the configuration statement is in effect indefinitely.

Format	absolute [start <i>time date month year</i>] [end <i>time date month year</i>]
Mode	Time-Range Config

no absolute

This command deletes the absolute time entry in the time range.

Format	no absolute
Mode	Time-Range Config

periodic

M4250

M4350

Use this command to add a periodic time entry to a time range. The *time* parameter is based off of the currently configured time zone.

The first occurrence of the *day-of-the-week* argument is the starting day(s) from which the configuration that referenced the time range starts going into effect. The second occurrence is the ending day or days from which the configuration that referenced the time range is no longer in effect. If the end days-of-the-week are the same as the start, they can be omitted

This argument can be any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday. Other possible values are:

- daily—Monday through Sunday
- weekdays—Monday through Friday

- weekend—Saturday and Sunday

If the ending days of the week are the same as the starting days of the week, they can be omitted.

The first occurrence of the *time* argument is the starting hours:minutes which the configuration that referenced the time range starts going into effect. The second occurrence of the *time* argument is the ending hours:minutes at which the configuration that referenced the time range is no longer in effect.

The hours:minutes are expressed in a 24-hour clock. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm.

Format	<code>periodic {{day-of-the-week time} {day-of-the-week [day-of-the-week]}} to {{day-of-the-week time} {day-of-the-week [day-of-the-week]}}</code>

Mode	Time-Range Config

no periodic

This command deletes a periodic time entry from a time range.

Format	<code>no periodic days-of-the-week time to time</code>

Mode	Time-Range Config

show time-range

M4250

M4350

Use this command to display a time range and all the absolute/periodic time entries that are defined for the time range. Use the *name* parameter to identify a specific time range to display. When *name* is not specified, all the time ranges defined in the system are displayed.

Format	<code>show time-range [name]</code>

Mode	Privileged EXEC

The information in the following table displays when no time range name is specified.

Term	Definition
Admin Mode	The administrative mode of the time range feature on the switch
Current number of all Time Ranges	The number of time ranges currently configured in the system.
Maximum number of all Time Ranges	The maximum number of time ranges that can be configured in the system.
Time Range Name	Name of the time range.

Term	Definition
Status	Status of the time range (active/inactive)
Periodic Entry count	The number of periodic entries configured for the time range.
Absolute Entry	Indicates whether an absolute entry has been configured for the time range (Exists).

Auto-Voice over IP Commands

This section describes the commands you use to configure Auto-Voice over IP (VoIP) commands. The Auto-VoIP feature explicitly matches VoIP streams in Ethernet switches and provides them with a better class-of-service than ordinary traffic. When you enable the Auto-VoIP feature on an interface, the interface scans incoming traffic for the following call-control protocols:

- Session Initiation Protocol (SIP)
- H.323
- Skinny Client Control Protocol (SCCP)

When a call-control protocol is detected, the switch assigns the traffic in that session to the highest CoS queue, which is generally used for time-sensitive traffic.

auto-voip

M4250

M4350

Use this command to configure auto VoIP mode. The supported modes are protocol-based and oui-based. Protocol-based auto VoIP prioritizes the voice data based on the layer 4 port used for the voice session. OUI based auto VoIP prioritizes the phone traffic based on the known OUI of the phone.

When both modes are enabled, if the connected phone OUI is one of the configured OUI, then the voice data is prioritized using OUI Auto VoIP, otherwise protocol-based Auto VoIP is used to prioritize the voice data.

Active sessions are cleared if protocol-based auto VoIP is disabled on the port.

Default	oui-based
Format	auto-voip [protocol-based oui-based]
Mode	Global Config Interface Config

no auto-voip

Use the **no** form of the command to set the default mode.

Format	no auto-voip [protocol-based oui-based]
Mode	Global Config Interface Config

auto-voip oui

M4250

M4350

Use this command to configure an OUI for Auto VoIP. The traffic from the configured OUI will get the highest priority over the other traffic. The *oui-prefix* is a unique OUI that identifies the device manufacturer or vendor. The OUI is specified in three octet values (each octets represented as two hexadecimal digits) separated by colons. The *oui-desc string* is a description of the OUI that identifies the manufacturer or vendor associated with the OUI.

Default	A list of known OUIs is present.
Format	auto-voip oui <i>oui-prefix</i> oui-desc <i>string</i>
Mode	Global Config

Command example:

The following example adds an OUI to the table:

```
(NETGEAR Switch) (Config)#auto-voip oui 00:03:6B oui-desc "ABC VoIPPhone"
```

no auto-voip oui

Use the **no auto-voip oui** command to remove a configured OUI prefix from the table.

Format	no auto-voip oui <i>oui-prefix</i>
Mode	Global Config

auto-voip oui-based priority

M4250

M4350

Use this command to configure the global OUI based auto VoIP priority. If the phone OUI matches one of the configured OUIs, the priority of traffic from the phone is changed to the OUI priority configured through this command. The *priority-value* is the 802.1p priority used for traffic that matches a value in the known OUI list. If the interface detects an OUI

match, the switch assigns the traffic in that session to the traffic class mapped to this priority value. Traffic classes with a higher value are generally used for time-sensitive traffic.

Default	Highest available priority.
Format	<code>auto-voip oui-based priority <i>priority-value</i></code>
Mode	Global Config

no auto-voip oui-based priority

Use the **no auto-voip oui-based priority** command to reset the global OUI based auto VoIP priority to its default.

Format	<code>no auto-voip oui-based priority</code>
Mode	Global Config

auto-voip protocol-based

M4250

M4350

Use this command to configure the global protocol-based auto VoIP remarking priority or traffic-class. If remark priority is configured, the voice data of the session is remarked with the priority configured through this command. The *remark-priority* is the 802.1p priority used for protocol-based VoIP traffic. If the interface detects a call-control protocol, the device marks traffic in that session with the specified 802.1p priority value (from 0 to 7) to ensure voice traffic always gets the highest priority throughout the network path.

The traffic class *value* is the traffic class used for protocol-based VoIP traffic. The value depends on the switch model:

- For an M4250 series switch, the range is from 0 to 7.
- For an M4350 series switch, the range is from 0 to 6.

If the interface detects a call-control protocol, the device assigns the traffic in that session to the configured Class of Service (CoS) queue. Traffic classes with a higher value are generally used for time-sensitive traffic. The CoS queue associated with the specified traffic class should be configured with the appropriate bandwidth allocation to allow priority treatment for VoIP traffic.

Note: You must enable tagging on auto VoIP-enabled ports to remark the voice data upon egress.

Default	Traffic class 7
Format	auto-voip protocol-based [remark <i>remark-priority</i> traffic-class <i>value</i>]
Mode	Global Config

no auto-voip protocol-based

Use this command to reset the global protocol based auto VoIP remarking priority or traffic-class to the default.

Format	no auto-voip protocol-based [remark <i>remark-priority</i> traffic-class <i>value</i>]
Mode	Global Config

auto-voip vlan

M4250

M4350

Use this command to configure the global Auto VoIP VLAN ID. The VLAN behavior is depend on the configured auto VoIP mode. The auto-VoIP VLAN is the VLAN used to segregate VoIP traffic from other non-voice traffic. All VoIP traffic that matches a value in the known OUI list gets assigned to this VoIP VLAN.

Default	None
Format	auto-voip vlan <i>vlan-id</i>
Mode	Global Config

no auto-voip vlan

Use the **no** form of the command to reset the auto-VoIP VLAN ID to the default value.

Format	no auto-voip vlan
Mode	Global Config

show auto-voip

M4250

M4350

Use this command to display the auto VoIP settings on one particular interface or on all interfaces of the switch. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

Format `show auto-voip [{protocol-based | oui-based} [interface {unit/slot/port | all}]`

Mode Privileged EXEC

Field	Description
VoIP VLAN ID	The global VoIP VLAN ID.
Prioritization Type	The type of prioritization used on voice traffic.
Class Value	• If the Prioritization Type is configured as traffic-class, then this value is the queue value. • If the Prioritization Type is configured as remark, then this value is 802.1p priority used to remark the voice traffic.
Priority	The 802.1p priority. This field is valid for OUI auto VoIP.
AutoVoIP Mode	The Auto VoIP mode on the interface.

Command example:

```
(NETGEAR Switch)# show auto-voip protocol-based interface all
```

```
VoIP VLAN Id..... 2
Prioritization Type..... traffic-class
Class Value..... 7
```

Interface	Auto VoIP Mode	Operational Status
0/1	Disabled	Down
0/2	Disabled	Down
0/3	Disabled	Down
0/4	Disabled	Down

Command example:

```
(NETGEAR Switch)# show auto-voip oui-based interface all
```

```
VoIP VLAN Id..... 2
Priority..... 7
Interface    Auto VoIP    Operational Status
              Mode
-----
0/1          Disabled    Down
0/2          Disabled    Down
0/3          Disabled    Down
0/4          Disabled    Down
0/5          Disabled    Down
```

show auto-voip oui-table

M4250

M4350

Use this command to display the VoIP OUI table information.

Format	show auto-voip oui-table

Mode	Privileged EXEC

Parameter	Description
OUI	OUI of the source MAC address.
Status	Default or configured entry.
OUI Description	Description of the OUI.

Command example:

```
(NETGEAR Switch)# show auto-voip oui-table
```

```
OUI          Status      Description
-----
00:01:E3     Default    SIEMENS
00:03:6B     Default    CISCO1
00:01:01     Configured VoIP phone
```

iSCSI Optimization Commands

Note: iSCSI optimization commands are supported on the M4350 series switches only. The M4250 series switches do not support iSCSI optimization.

This section describes commands you use to monitor iSCSI sessions and prioritize iSCSI packets. iSCSI Optimization provides a means of giving traffic between iSCSI initiator and target systems special Quality of Service (QoS) treatment. This is accomplished by monitoring traffic to detect packets used by iSCSI stations to establish 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.

iscsi aging time

M4350

This command sets the aging time for iSCSI sessions. Behavior when changing aging time:

- When aging time is increased, current sessions will be timed out according to the new value.
- When aging time is decreased, any sessions that have been dormant for a time exceeding the new setting will be immediately deleted from the table. All other sessions will continue to be monitored against the new time out value.

Default	10 minutes
Format	<code>iscsi aging time time</code>
Mode	Global Config

Parameter	Description
time	The number of minutes a session must be inactive prior to its removal. Range: 1-43,200.

Command example:

The following example sets the aging time for iSCSI sessions to 100 minutes:

```
(NETGEAR Switch) (config)#iscsi aging time 100
```

no iscsi aging time

Use the **no iscsi aging time** command to reset the aging time value to the default value.

Format	no iscsi aging time

Mode	Global Config

iscsi cos

M4350

This command sets the quality of service profile that will be applied to iSCSI flows. iSCSI flows are assigned by default to the highest VPT or DSCP mapped to the highest queue not used for switch management. Take care that you configure the relevant Class of Service parameters for the queue in order to complete the setting.

Setting the VPT or 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).

You can complete the QoS setting by configuring the relevant ports to work in other scheduling and queue management modes via the Class of Service settings. Depending on the platform, these choices may 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 may get starved. In WRR the queue to which the flow is assigned to can be set to get the required percentage.

iSCSI optimization is best applied to mixed-traffic networks in which iSCSI packets constitute a portion of overall traffic. In these cases, the assignment of iSCSI packets to nondefault queues can provide flows with lower latency and prevent queue resource contention.

If iSCSI frames comprise most of the traffic passing through the switch, the system provides optimal throughput if all traffic is assigned to the default queue. An example of this situation is a Storage Area Network (SAN) in which the switch is dedicated to interconnecting iSCSI targets with initiators. Using the default queue for this homogenous traffic provides the best performance in traffic-burst handling and the most accurate 802.3x Flow Control Pause Frame generation. In these cases, iSCSI Flow Acceleration, which can assign iSCSI frames to queues other than the default queue, might result in lower overall throughput or increased packet loss.

Format	iscsi cos {vpt vpt dscp dscp} [remark]

Mode	Global Config

Parameter	Description
vpt or dscp	The VLAN Priority Tag or DSCP to assign iSCSI session packets.
remark	Mark the iSCSI frames with the configured VPT or DSCP when egressing the switch.

Command example:

The following example sets the quality of service profile that is applied to iSCSI flows:

```
(NETGEAR Switch) (config) #iscsi cos vpt 5 remark
```

```
no iscsi cos
```

Use the **no iscsi cos** command to return to the default.

Format	no iscsi cos

Mode	Global Config

```
iscsi cos enable
```

M4350

This command enables the assignment of iSCSI flows that you can configure with the **iscsi cos** command.

Format	iscsi cos enable

Mode	Global Config

```
no iscsi cos enable
```

This command disables the assignment of iSCSI flows.

Format	no iscsi cos enable

Mode	Global Config

```
iscsi enable
```

M4350

This command globally enables iSCSI awareness.

Default	disabled

Format	iscsi enable

Mode	Global Config

Command example:

The following example enables iSCSI awareness:

```
(NETGEAR Switch) (config) #iscsi enable
```

no iscsi enable

This command disables iSCSI awareness. When you use the **no iscsi enable** command, iSCSI resources are released.

Format	no iscsi enable

Mode	Global Config

iscsi target port

M4350

This command configures an iSCSI target port and, optionally, a target system's IP address and IQN name. When working with private iSCSI ports (not IANA-assigned ports 3260/860), it is recommended to specify the target IP address as well, so that the switch will only snoop frames with which the TCP destination port is one of the configured TCP ports, and the destination IP is the target's IP address. This way the CPU will not be falsely loaded by non-iSCSI flows (if by chance other applications also choose to use these un-reserved ports).

When a port is already defined and not bound to an IP address, and you want to bind it to an IP address, first remove it by using the **no** form of the command and then add it again, this time together with the relevant IP address.

Target names are only for display when using the **show iscsi** command. These names are not used to match with the iSCSI session information acquired by snooping.

A maximum of 16 TCP ports can be configured either bound to IP or not.

Default	iSCSI well-known ports 3260 and 860 are configured as default but can be removed as any other configured target.

Format	iscsi target port <i>tcp-port-1</i> [<i>tcp-port-2...tcp-port-16</i>] [<i>address ip-address</i>] [<i>name targetname</i>]

Mode	Global Config

Parameter	Description
tcp-port-n	TCP port number or list of TCP port numbers on which the iSCSI target listens to requests. Up to 16 TCP ports can be defined in the system in one command or by using multiple commands.
ip-address	IP address of the iSCSI target. When the no form of this command is used, and the tcp port to be deleted is one bound to a specific IP address, the address field must be present.
targetname	iSCSI name of the iSCSI target. The name can be statically configured; however, it can be obtained from iSNS or from sendTargets response. The initiator must present both its iSCSI Initiator Name and the iSCSI Target Name to which it wishes to connect in the first login request of a new session or connection.

Command example:

The following example configures TCP Port 49154 to target IP address 172.16.1.20:

```
(NETGEAR Switch) (config)#iscsi target port 49154 address 172.16.1.20
```

no iscsi target port

Use the **no iscsi target port** command to delete an iSCSI target port, address, and name.

Format	no iscsi target port
Mode	Global Config

show iscsi

M4350

This command displays the iSCSI settings.

Format	show iscsi
Mode	Privileged EXEC

Command example:

The following example shows the default configuration:

```
(NETGEAR Switch)#show iscsi
iSCSI disabled
iSCSI vpt is 5, remark
Session aging time: 10 min
Maximum number of sessions is 192
-----
iSCSI Targets and TCP ports:
-----
TCP      Port      Target IP Address      Name
      860      Not Configured         Not Configured
      3260     Not Configured         Not Configured
```

Command example:

The following example enable iSCSI:

```
(NETGEAR Switch)#configure
(NETGEAR Switch) (config)#iscsi enable
```

Command example:

The following examples shows that iSCSI sessions and connections are established using TCP ports 3260 or 860. Packets sent on detected iSCSI TCP connections are assigned to traffic class 2 (see the CoS configuration shown below). Because remark is enabled, the packets are marked with IEEE 802.1p priority to 5 before transmission.

```
(NETGEAR Switch)#show iscsi
iscsi enabled
```



```
iSCSI vpt is 5, remark
Session aging time: 10 min
Maximum number of sessions is 192
```

```
-----
iSCSI Targets and TCP ports:
```

```
-----
TCP      Port      Target IP Address      Name
      860      Configured              Not Configured
      3260     Configured              Not Configured
```

```
(NETGEAR Switch)#show classofservice dot1p-mapping
```

```
User Priority      Traffic Class
-----
          0              1
          1              0
          2              0
          3              1
          4              2
          5              2
          6              3
          6              3
```

show iscsi sessions

M4350

This command displays the iSCSI sessions.

Default	If not specified, sessions are displayed in short mode (not detailed).
Format	show iscsi sessions [detailed]
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) # show iscsi sessions
Target: iqn.1993-11.com.disk-vendor:diskarrays.sn.45678
-----
Initiator: iqn.1992-04.com.os-vendor.plan9:cdrom.12
ISID: 11
Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10
ISID: 222
-----
Target: iqn.103-1.com.storage-vendor:sn.43338.
storage.tape:sys1.xyz
Session 3:
Initiator: iqn.1992-04.com.os-vendor.plan9:cdrom.12
```

Session 4:

Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10

Command example:

(NETGEAR Switch)# show iscsi sessions detailed

Target: iqn.1993-11.com.disk-vendor:diskarrays.sn.45678

Session 1:

Initiator: iqn.1992-04.com.os

vendor.plan9:cdrom.12.storage:sys1.xyz

Time started: 17-Jul-2008 10:04:50

Time for aging out: 10 min

ISID: 11

Initiator	Initiator	Target	Target
IP address	TCP port	IP address	IP port
172.16.1.3	49154	172.16.1.20	30001
172.16.1.4	49155	172.16.1.21	30001
172.16.1.5	49156	172.16.1.22	30001

Session 2:

Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10

Time started: 17-Aug-2008 21:04:50

Time for aging out: 2 min

ISID: 22

Initiator	Initiator	Target	Target
IP address	TCP port	IP address	IP port
172.16.1.30	49200	172.16.1.20	30001
172.16.1.30	49201	172.16.1.21	30001

12

IP Multicast Commands

This chapter describes the IP multicast commands. The chapter contains the following sections:

- [Multicast Commands](#)
- [DVMRP Commands](#)
- [PIM Commands](#)
- [Internet Group Message Protocol Commands](#)
- [IGMP Proxy Commands](#)

The commands in this chapter are in one of two functional groups:

- **Show commands.** Display switch settings, statistics, and other information.
- **Configuration commands.** Configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.

Multicast Commands

This section describes the commands you use to configure IP Multicast and to view IP Multicast settings and statistics.

ip mcast boundary

M4250

M4350

This command adds an administrative scope multicast boundary specified by *groupipaddr* and *mask* for which this multicast administrative boundary is applicable. *groupipaddr* is a group IP address and *mask* is a group IP mask. This command can be used to configure a single interface or a range of interfaces.

Format	<code>ip mcast boundary groupipaddr mask</code>
Mode	Interface Config

no ip mcast boundary

This command deletes an administrative scope multicast boundary specified by *groupipaddr* and *mask* for which this multicast administrative boundary is applicable. *groupipaddr* is a group IP address and *mask* is a group IP mask.

Format	<code>no ip mcast boundary groupipaddr mask</code>
Mode	Interface Config

ip mroute

M4250

M4350

This command configures an IPv4 multicast static route for a source.

Default	No MRoute is configured on the system.
Format	<code>ip mroute src-ip-addr src-mask rpf-addr preference</code>
Mode	Global Config

Parameter	Description
src-ip-addr	The IP address of the multicast source network.
src-mask	The IP mask of the multicast data source.

Parameter	Description
rpf-ip-addr	The IP address of the RPF next-hop router toward the source.
preference	The administrative distance for this Static MRoute, that is, the preference value. The range is 1 to 255.

no ip mroute

This command removes the configured IPv4 multicast static route.

Format	<code>no ip mroute src-ip-addr</code>
Mode	Global Config

ip mroute static-multicast

M4250

M4350

This command configures a static multicast route for a multicast group IP address and a list of VLANs that are enabled for routing.

Default	No default static routes
Format	<code>ip mroute static-multicast group-ip-address vlan-list</code>
Mode	Global Config

Parameters	Description
group-ip-address	A multicast group IP address.
vlan-list	A list of VLANs in the range of 1 to 4093. Each VLAN ID must be separated by a comma.

Note the following requirements:

- All VLANs that you specify in the list must be enabled for routing with an IP address configured.
- You cannot configure two static multicast routes with the same group IP address, even though the VLAN lists differ. If you must change the VLAN list for a static route, delete the existing static route and create a new one with an updated VLAN list.

Command example:

To install a static route for multicast group address 224.0.1.129 for VLANs 1, 2, 3, and 4, enter the following command:

```
(config)#ip mroute static-multicast 224.0.1.129 1,2,3,4
```

no ip mroute static-multicast

This command removes a static multicast route for a group IP address.

The *group-ip-address* argument represents the multicast group IP address.

Format	no ip mroute static-multicast <i>group-ip-address</i>
Mode	Global Config

ip multicast

M4250

M4350

This command sets the administrative mode of the IP multicast forwarder in the router to active.

Default	disabled
Format	ip multicast
Mode	Global Config

no ip multicast

This command sets the administrative mode of the IP multicast forwarder in the router to inactive.

Format	no ip multicast
Mode	Global Config

ip multicast ttl-threshold

M4250

M4350

This command is specific to IPv4. Use this command to apply a time-to-live (TTL) threshold value to a routing interface or range of interfaces. The *ttlvalue* is the TTL threshold that is be applied to multicast data packets that are forwarded from the interface. This command sets the TTL threshold value so that data packets with a TTL value above the configured value are dropped form the interface. The value for *ttlvalue* ranges from 0 to 255.

Default	1
Format	ip multicast ttl-threshold <i>ttlvalue</i>
Mode	Interface Config

no ip multicast ttl-threshold

This command applies the default TTL threshold to a routing interface. The TTL threshold is applied to the multicast data packets that are forwarded from the interface.

Format	no ip multicast ttl-threshold

Mode	Interface Config

show ip mcast

M4250

M4350

This command displays the system-wide multicast information.

Format	show ip mcast

Modes	Privileged EXEC User EXEC

Term	Definition
Admin Mode	The administrative status of multicast. Possible values are enabled or disabled.
Protocol State	The current state of the multicast protocol. Possible values are Operational or Non-Operational.
Table Max Size	The maximum number of entries allowed in the multicast table.
Protocol	The multicast protocol running on the router. Possible values are PIMDM, PIMSM, or DVMRP.
Multicast Forwarding Cache Entry Count	The number of entries in the multicast forwarding cache.

show ip mcast boundary

M4250

M4350

This command displays all the configured administrative discovered multicast boundaries.

The interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN directly. The *vlan-id* parameter is a number in the range of 1–4093.

Format	<code>show ip mcast boundary {unit/slot/port vlan vlan-id all}</code>
Modes	Privileged EXEC User EXEC
Term	Definition
Interface	The interface.
Group Ip	The group IP address.
Mask	The group IP mask.

show ip mcast interface

M4250

M4350

This command displays the multicast information for the specified interface.

The interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

Format	<code>show ip mcast interface {unit/slot/port vlan vlan-id}</code>
Modes	Privileged EXEC User EXEC
Term	Definition
Interface	<i>unit/slot/port</i>
TTL	The time-to-live value for this interface.

show ip mroute

M4250

M4350

This command displays a summary or all the details of the multicast table.

Format	show ip mroute {detail summary}
Modes	Privileged EXEC User EXEC

If you use the **detail** parameter, the command displays the following fields.

Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Expiry Time	The time of expiry of this entry in seconds.
Up Time	The time elapsed since the entry was created in seconds.
RPF Neighbor	The IP address of the RPF neighbor.
Flags	The flags associated with this entry.

If you use the **summary** parameter, the command displays the following fields.

Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which the entry was created.
Incoming Interface	The interface on which the packet for the source/group arrives.
Outgoing Interface List	The list of outgoing interfaces on which the packet is forwarded.

show ip mroute group

M4250**M4350**

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast route table containing the specified group address (*groupipaddr*).

Format	<code>show ip mroute group <i>groupipaddr</i> {detail summary}</code>
Modes	Privileged EXEC User EXEC
Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which this entry was created.
Incoming Interface	The interface on which the packet for this group arrives.
Outgoing Interface List	The list of outgoing interfaces on which this packet is forwarded.

show ip mroute source

M4250**M4350**

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast route table containing the specified source IP address (*sourceipaddr*).

Format	<code>show ip mroute source <i>sourceipaddr</i> {detail summary}</code>
Modes	Privileged EXEC User EXEC

If you use the *sourceipaddr* parameter, the command displays the following column headings in the output table.

Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Expiry Time	The time of expiry of this entry in seconds.

Term	Definition
Up Time	The time elapsed since the entry was created in seconds.
RPF Neighbor	The IP address of the RPF neighbor.
Flags	The flags associated with this entry.

If you use the **summary** parameter, the command displays the following column headings in the output table.

Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which this entry was created.
Incoming Interface	The interface on which the packet for this source arrives.
Outgoing Interface List	The list of outgoing interfaces on which this packet is forwarded.

show ip mroute static

M4250

M4350

Use this command in Privileged EXEC or User EXEC mode to display all the static routes configured in the static mcast table, if it is specified, or display the static route associated with the particular *sourceipaddr*.

Format	show ip mroute static [<i>sourceipaddr</i>]
Modes	Privileged EXEC User EXEC

Parameter	Description
Source IP	IP address of the multicast source network.
Source Mask	The subnetwork mask pertaining to the sourceIP.
RPF Address	The IP address of the RPF next-hop router toward the source.
Preference	The administrative distance for this Static MRoute.

Command example:

```
console#show ip mroute static
```

```

                MULTICAST STATIC ROUTES
Source IP      Source Mask    RPF Address    Preference
-----
1.1.1.1        255.255.255.0    2.2.2.2        23

```

show ip mroute static-multicast**M4250****M4350**

Use this command in Privileged EXEC or User EXEC mode to display the manually added static multicast routes.

Format	show ip mroute static-multicast

Modes	Privileged EXEC User EXEC

Parameter	Description
Maximum Multicast Static Address Count	The maximum number of allowed static multicast routes.
Current Multicast Static Address Count	The number of configured static multicast routes.
Group Address	The configured multicast group IP address.
Egress VLAN List	The VLANs that are associated with the static multicast route.

Command example:

```
(NETGEAR Switch) #show ip mroute static-multicast
```

```

Maximum Multicast Static Address Count ..... 32
Current Multicast Static Address Count ..... 4

```

```

Group Address      Egress VLAN List
-----
225.1.1.1          1-2
225.1.1.5          1
225.1.1.2          1-2
225.1.1.3          1

```

clear ip mroute

M4250

M4350

This command deletes all or the specified IP multicast route entries. This command clears only dynamic mroute entries. It does not clear static mroutes.

Format	<code>clear ip mroute { * <i>group-address</i> [<i>source-address</i>] }</code>

Modes	Privileged EXEC

Parameter	Description
*	Deletes all IPv4 entries from the IP multicast routing table.
group-address	IP address of the multicast group.
source-address	The optional IP address of a multicast source that is sending multicast traffic to the group.

Command example:

The following example deletes all entries from the IP multicast routing table:

```
(NETGEAR Switch) # clear ip mroute *
```

Command example:

The following example deletes all entries from the IP multicast routing table that match the multicast group address (224.1.2.1), irrespective of which source is sending for this group:

```
(NETGEAR Switch) # clear ip mroute 224.1.2.1
```

Command example:

The following example deletes all entries from the IP multicast routing table that match the multicast group address (224.1.2.1) and the multicast source address (192.168.10.10):

```
(NETGEAR Switch) # clear ip mroute 224.1.2.1 192.168.10.10
```

DVMRP Commands

Note: Distance Vector Multicast Routing Protocol (DVMRP) commands are supported on the M4350 series switches only. The M4250 series switches do not support DVMRP.

This section describes the Distance Vector Multicast Routing Protocol (DVMRP) commands.

ip dvmrp (Global Config)

M4350

This command sets administrative mode of DVMRP in the router to active.

Default	disabled
Format	ip dvmrp
Mode	Global Config

no ip dvmrp

This command sets administrative mode of DVMRP in the router to inactive.

Format	no ip dvmrp
Mode	Global Config

ip dvmrp metric (Global Config)

M4350

This command configures the metric for an interface or range of interfaces. This value is used in the DVMRP messages as the cost to reach this network. The *metric* argument is a value in the range from 1 to 31.

Default	1
Format	ip dvmrp [metric <i>metric</i>]
Mode	Interface Config

no ip dvmrp metric (Global Config)

This command resets the metric for an interface to the default value. This value is used in the DVMRP messages as the cost to reach this network.

Format	no ip dvmrp [metric]

Mode	Interface Config

ip dvmrp trapflags

M4350

This command enables the DVMRP trap mode.

Default	disabled

Format	ip dvmrp trapflags

Mode	Global Config

no ip dvmrp trapflags

This command disables the DVMRP trap mode.

Format	no ip dvmrp trapflags

Mode	Global Config

ip dvmrp (Interface Config)

M4350

This command sets the administrative mode of DVMRP on an interface or range of interfaces to active.

Default	disabled

Format	ip dvmrp

Mode	Interface Config

no ip dvmrp (Interface Config)

This command sets the administrative mode of DVMRP on an interface to inactive.

Format	no ip dvmrp

Mode	Interface Config

show ip dvmrp

M4350

This command displays the system-wide information for DVMRP.

Format	<code>show ip dvmrp</code>
Modes	Privileged EXEC User EXEC

Term	Definition
Admin Mode	Indicates whether DVMRP is enabled or disabled.
Version String	The version of DVMRP being used.
Number of Routes	The number of routes in the DVMRP routing table.
Reachable Routes	The number of entries in the routing table with non-infinite metrics.

The following fields are displayed for each interface.

Term	Definition
Interface	<code>unit/slot/port</code>
Interface Mode	The mode of this interface. Possible values are Enabled and Disabled.
State	The current state of DVMRP on this interface. Possible values are Operational or Non-Operational.

show ip dvmrp interface

M4350

This command displays the interface information for DVMRP on the specified interface.

The argument `unit/slot/port` corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and `vlan-id` parameter are used to specify the VLAN ID of the routing VLAN. The `vlan-id` parameter is a number in the range of 1–4093.

Format	<code>show ip dvmrp interface {unit/slot/port vlan vlan-id}</code>
Modes	Privileged EXEC User EXEC

Term	Definition
Interface Mode	Indicates whether DVMRP is enabled or disabled on the specified interface.
Metric	The metric of this interface. This is a configured value.
Local Address	The IP address of the interface.

The following field is displayed only when DVMRP is operational on the interface.

Term	Definition
Generation ID	The Generation ID value for the interface. This is used by the neighboring routers to detect that the DVMRP table should be resent.

The following fields are displayed only if DVMRP is enabled on this interface.

Term	Definition
Received Bad Packets	The number of invalid packets received.
Received Bad Routes	The number of invalid routes received.
Sent Routes	The number of routes that have been sent on this interface.

show ip dvmrp neighbor

M4350

This command displays the neighbor information for DVMRP.

Format	show ip dvmrp neighbor
Modes	Privileged EXEC User EXEC

Term	Definition
IfIndex	The value of the interface used to reach the neighbor.
Nbr IP Addr	The IP address of the DVMRP neighbor for which this entry contains information.
State	The state of the neighboring router. The possible value for this field are ACTIVE or DOWN.
Up Time	The time since this neighboring router was learned.
Expiry Time	The time remaining for the neighbor to age out. This field is not applicable if the State is DOWN.
Generation ID	The Generation ID value for the neighbor.
Major Version	The major version of DVMRP protocol of neighbor.
Minor Version	The minor version of DVMRP protocol of neighbor.
Capabilities	The capabilities of neighbor.
Received Routes	The number of routes received from the neighbor.
Rcvd Bad Pkts	The number of invalid packets received from this neighbor.
Rcvd Bad Routes	The number of correct packets received with invalid routes.

show ip dvmrp nexthop

M4350

This command displays the next hop information on outgoing interfaces for routing multicast datagrams.

Format	show ip dvmrp nexthop
Modes	Privileged EXEC User EXEC
Term	Definition
Source IP	The sources for which this entry specifies a next hop on an outgoing interface.
Source Mask	The IP Mask for the sources for which this entry specifies a next hop on an outgoing interface.
Next Hop Interface	The interface in <i>unit/slot/port</i> format for the outgoing interface for this next hop.
Type	The network is a LEAF or a BRANCH.

show ip dvmrp prune

M4350

This command displays the table listing the router's upstream prune information.

Format	show ip dvmrp prune
Modes	Privileged EXEC User EXEC
Term	Definition
Group IP	The multicast Address that is pruned.
Source IP	The IP address of the source that has pruned.
Source Mask	The network Mask for the prune source. It should be all 1s or both the prune source and prune mask must match.
Expiry Time (secs)	The expiry time in seconds. This is the time remaining for this prune to age out.

show ip dvmrp route

M4350

This command displays the multicast routing information for DVMRP.

Format	show ip dvmrp route
Modes	Privileged EXEC User EXEC

Term	Definition
Source Address	The multicast address of the source group.
Source Mask	The IP Mask for the source group.
Upstream Neighbor	The IP address of the neighbor which is the source for the packets for a specified multicast address.
Interface	The interface used to receive the packets sent by the sources.
Metric	The distance in hops to the source subnet. This field has a different meaning than the Interface Metric field.
Expiry Time (secs)	The expiry time in seconds, which is the time left for this route to age out.
Up Time (secs)	The time when a specified route was learnt, in seconds.

PIM Commands

This section describes the commands you use to configure Protocol Independent Multicast -Dense Mode (PIM-DM) and Protocol Independent Multicast - Sparse Mode (PIM-SM). PIM-DM and PIM-SM are multicast routing protocols that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol. Only one PIM mode can be operational at a time.

ip pim dense

M4250

M4350

This command administratively enables the PIM Dense mode across the router.

Default	disabled
Format	ip pim dense
Mode	Global Config

Command example:

```
(NETGEAR) (Config) #ip pim dense
```

no ip pim dense

This command administratively disables the PIM Dense mode across the router.

Format	no ip pim dense
Mode	Global Config

ip pim sparse

M4250

M4350

This command administratively enables the PIM Sparse mode across the router.

Default	disabled
Format	ip pim sparse
Mode	Global Config

Command example:

```
(NETGEAR) (Config) #ip pim sparse
```

no ip pim sparse

This command administratively disables the PIM Sparse mode across the router.

Format	no ip pim sparse
Mode	Global Config

ip pim

M4250

M4350

Use this command to administratively enable PIM on the specified interface.

Default	disabled
Format	ip pim
Mode	Interface Config

Command example:

```
(NETGEAR) (Interface 1/0/1) #ip pim
```

no ip pim

Use this command to disable PIM on the specified interface.

Format	no ip pim
Mode	Interface Config

ip pim hello-interval

M4250**M4350**

This command configures the transmission frequency of PIM hello messages the specified interface. The *seconds* argument is a value in a range of 0 to 18000 seconds.

Default	30
Format	ip pim hello-interval <i>seconds</i>
Mode	Interface Config

Command example:

```
(NETGEAR) (Interface 1/0/1) #ip pim hello-interval 50
```

no ip pim hello-interval

This command resets the transmission frequency of hello messages between PIM enabled neighbors to the default value.

Format	no ip pim hello-interval
Mode	Interface Config

ip pim bsr-border

M4250**M4350**

Use this command to prevent bootstrap router (BSR) messages from being sent or received on the specified interface.

Note: This command takes effect only when Sparse mode is enabled in the Global mode.

Default	disabled
Format	ip pim bsr-border
Mode	Interface Config

Command example:

```
(NETGEAR) (Interface 1/0/1) #ip pim bsr-border
```

no ip pim bsr-border

Use this command to disable the specified interface from being the BSR border.

Format	no ip pim bsr-border
Mode	Interface Config

ip pim bsr-candidat

M4250

M4350

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR).

The argument for an interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command description and format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default	Disabled

Format	ip pim bsr-candidate interface { <i>unit/slot/port</i> <i>vlan vlan-id</i> } <i>hash-mask-length</i> [<i>bsr-priority</i>] [<i>interval interval</i>]

Mode	Global Config

Parameters	Description
slot/port or unit/slot/port or vlan-id	Interface or VLAN number on this router from which the BSR address is derived, to make it a candidate. This interface or VLAN must be enabled with PIM.
hash-mask-length	Length of a mask (32 bits maximum) that is to be “ANDed” with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This allows you to get one RP for multiple groups.

Parameters	Description
bsr-priority	[Optional] Priority of the candidate BSR. The range is an integer from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR. The default value is 0.
interval	[Optional] Indicates the BSR candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.

Command example: The following shows examples of the command.

```
(NETGEAR) (Config) #ip pim bsr-candidate interface 1/0/1 32 5
(NETGEAR) (Config) #ip pim bsr-candidate interface 1/0/1 32 5 interval 100
```

no ip pim bsr-candidate

Use this command to remove the configured PIM Candidate BSR router.

Format	no ip pim bsr-candidate interface {unit/slot/port vlan vlan-id}
Mode	Global Config

ip pim dr-priority

M4250

M4350

Use this command to set the priority value for which a router is elected as the designated router (DR). The *priority* argument is a value in the range of 0–2147483647.

Note: This command takes effect only when Sparse mode is enabled in the Global mode.

Default	1
Format	ip pim dr-priority <i>priority</i>
Mode	Interface Config

Command example:

```
(NETGEAR) (Interface 1/0/1) #ip pim dr-priority 10
```

no ip pim dr-priority

Use this command to return the DR Priority on the specified interface to its default value.

Format	no ip pim dr-priority
Mode	Interface Config

ip pim join-prune-interval

M4250

M4350

Use this command to configure the frequency of PIM Join/Prune messages on a specified interface. The join/prune interval is specified in seconds. The *seconds* argument can be configured as a value from 0 to 18000 seconds.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default	60
Format	ip pim join-prune-interval <i>seconds</i>
Mode	Interface Config

Command example:

```
(NETGEAR) (Interface 1/0/1) #ip pim join-prune-interval 90
```

no ip pim join-prune-interval

Use this command to set the join/prune interval on the specified interface to the default value.

Format	no ip pim join-prune-interval
Mode	Interface Config

ip pim rp-address

M4250

M4350

This command defines the address of a PIM Rendezvous point (RP) for a specific multicast group range.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default	0
Format	<code>ip pim rp-address <i>rp-address</i> {<i>group-address group-mask</i> <i>prefix-list list-name</i>} [<i>override</i>]</code>
Mode	Global Config

Parameter	Description
rp-address	The IP address of the RP.
group-address	The group address supported by the RP.
group-mask	The group mask for the group address.
list-name	The name of a list that contains group ranges for the RP.
override	[Optional] Indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

Command example:

```
(NETGEAR) (Config) #ip pim rp-address 192.168.10.1
224.1.2.0 255.255.255.0
```

no ip pim rp-address

Use this command to remove the address of the configured PIM Rendezvous point (RP) for the specified multicast group range.

Format	<code>no ip pim rp-address <i>rp-address</i> {<i>group-address group-mask</i> <i>prefix-list list-name</i>}</code>
Mode	Global Config

ip pim rp-candidate

M4250

M4350

Use this command to configure the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR) for a specific multicast group range.

The interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default	Disabled
Format	<code>ip pim rp-candidate interface {unit/slot/port vlan vlan-id} group-address group-mask [interval interval] [priority value]</code>
Mode	Global Config

Parameter	Description
slot/port or unit/slot/port or vlan-id	The interface or the VLAN ID is advertised as a candidate RP address. This interface or VLAN must be enabled with PIM.
group-address	The multicast group address that is advertised in association with the RP address.
group-mask	The multicast group prefix that is advertised in association with the RP address.
interval	[Optional] Indicates the RP candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.
value	[Optional] Indicates the RP candidate advertisement priority value. The range is from 0 to 255.

Command example: The following shows examples of the command.

```
(NETGEAR) (Config) #ip pim rp-candidate interface 1/0/1 224.1.2.0 255.255.255.0
(NETGEAR) (Config) #ip pim rp-candidate interface 1/0/1 224.1.2.0 255.255.255.0 interval 200
```

no ip pim rp-candidate

Use this command to remove the configured PIM candidate Rendezvous point (RP) configuration for a specific multicast group range.

Format	no ip pim rp-candidate interface { <i>unit/slot/port</i> <i>vlan vlan-id</i> } <i>group-address group-mask</i> [<i>interval</i>] [<i>priority</i>]
Mode	Global Config

ip pim ssm

M4250

M4350

Use this command to define the Source Specific Multicast (SSM) range of IP multicast addresses on the router.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default	disabled

Format	ip pim ssm { <i>default</i> <i>group-address group-mask</i> }

Mode	Global Config

Parameter	Description

default	Defines the SSM range access list to 232/8.

Command example:

```
(NETGEAR) (Config) #ip pim ssm default
(NETGEAR) (Config) #ip pim ssm 232.1.2.0 255.255.255.0
```

no ip pim ssm

Use this command to remove the Source Specific Multicast (SSM) range of IP multicast addresses on the router.

Format	no ip pim ssm { <i>default</i> <i>group-address group-mask</i> }
Mode	Global Config

ip pim-trapflags

M4250**M4350**

This command enables the PIM trap mode for both Sparse Mode (SM) and Dense Mode (DM).

Default	disabled
Format	ip pim-trapflags
Mode	Global Config

no ip pim-trapflags

This command sets the PIM trap mode to the default.

Format	no ip pim-trapflags
Mode	Global Config

show ip mfc

M4250**M4350**

This command displays multicast route entries in the multicast forwarding (MFC) database.

Format	show ip mfc
Modes	Privileged EXEC User EXEC

Term	Definition
MFC IPv4 Mode	Indicates whether IPv4 multicast routing is operational.
MFC IPv6 Mode	Indicates whether IPv6 Multicast routing is operational.
MFC Entry Count	The number of entries present in MFC.
Current multicast IPv4 Protocol	The current operating IPv4 multicast routing protocol.
Current multicast IPv6 Protocol	The current operating multicast IPv6 routing protocol.
Total Software Forwarded packets	The total number of multicast packets forwarded in software.
Source Address	The source address of the multicast route entry.
Group Address	The group address of the multicast route entry.

Term	Definition
Packets Forwarded in Software for this entry	The number of multicast packets that are forwarded in software for a specific multicast route entry.
Protocol	The multicast routing protocol that added a specific entry
Expiry Time (secs)	The expiration time in seconds for a specific multicast route entry.
Up Time (secs)	The up time in seconds for a specific multicast routing entry.
Incoming interface	The incoming interface for a specific multicast route entry.
Outgoing interface list	The outgoing interface list for a specific multicast route entry.

Command example:

```
(NETGEAR) #show ip mfc
```

```

MFC IPv4 Mode..... Enabled
MFC IPv6 Mode..... Disabled
MFC Entry Count ..... 1
Current multicast IPv4 protocol..... PIMSM
Current multicast IPv6 protocol..... No protocol enabled.
Total software forwarded packets ..... 0
Source address: 192.168.10.5
Group address: 225.1.1.1
Packets forwarded in software for this entry: 0          Protocol: PIM-SM
Expiry Time (secs): 206          Up Time (secs): 4
Incoming interface: 1/0/10      Outgoing interface list: None

```

show ip pim**M4250****M4350**

This command displays the system-wide information for PIM-DM or PIM-SM.

Format	show ip pim
Modes	Privileged EXEC User EXEC

Note: If the PIM mode is PIM-DM (dense), some of the fields in the following table do not display in the command output because they are applicable only to PIM-SM.

Term	Definition
PIM Mode	Indicates the configured mode of the PIM protocol as dense (PIM-DM) or sparse (PIM-SM)
Interface	The interface.
Interface Mode	Indicates whether PIM is enabled or disabled on this interface.
Operational Status	The current state of PIM on this interface: Operational or Non-Operational.

The following example shows PIM Mode - Dense:

```
(NETGEAR) #show ip pim
```

```
PIM Mode Dense
```

Interface	Interface-Mode	Operational-Status
-----	-----	-----
1/0/1	Enabled	Operational
1/0/3	Disabled	Non-Operational

Command example:

The following example shows PIM Mode - Sparse

```
(NETGEAR) #show ip pim
```

```
PIM Mode Sparse
```

Interface	Interface-Mode	Operational-Status
-----	-----	-----
1/0/1	Enabled	Operational
1/0/3	Disabled	Non-Operational

Command example:

The following example shows that PIM is not configured:

```
(NETGEAR) #show ip pim
```

```
PIM Mode None
```

```
None of the routing interfaces are enabled for PIM.
```

show ip pim ssm

M4250

M4350

This command displays the configured source specific IP multicast addresses.

Format	show ip pim ssm
Modes	Privileged EXEC User EXEC
Term	Definition
Group Address	The IP multicast address of the SSM group.
Prefix Length	The network prefix length.

Command example:

```
(NETGEAR) #show ip pim ssm
Group Address/Prefix Length
-----
232.0.0.0/8
```

Command example:

If no SSM group range is configured, the command displays the following message:

```
No SSM address range is configured.
```

show ip pim interface

M4250

M4350

This command displays the PIM interface status parameters.

The interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

If no interface is specified, the command displays the status parameters of all PIM-enabled interfaces.

Fully Managed Switches M4250 and M4350 Series

Format	<code>show ip pim interface [unit/slot/port vlan vlan-id]</code>
Modes	Privileged EXEC User EXEC

Term	Definition
Interface	The interface number.
Mode	Indicates the active PIM mode enabled on the interface is dense or sparse.
Hello Interval	The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.
Join Prune Interval	The join/prune interval value for the PIM router. The interval is in seconds.
DR Priority	The priority of the Designated Router configured on the interface. This field is not applicable if the interface mode is Dense.
BSR Border	Identifies whether this interface is configured as a bootstrap router border interface.
Neighbor Count	The number of PIM neighbors learned on this interface. This is a dynamic value and is shown only when a PIM interface is operational.
Designated Router	The IP address of the elected Designated Router for this interface. This is a dynamic value and will only be shown when a PIM interface is operational. This field is not applicable if the interface mode is Dense.

Command example:

```
(NETGEAR) #show ip pim interface
```

```
Interface.....1/0/1
  Mode.....Sparse
  Hello Interval (secs).....30
  Join Prune Interval (secs).....60
  DR Priority.....1
  BSR Border.....Disabled
  Neighbor Count.....1
  Designated Router.....192.168.10.1

Interface.....1/0/2
  Mode.....Sparse
  Hello Interval (secs).....30
  Join Prune Interval (secs).....60
  DR Priority.....1
  BSR Border.....Disabled
  Neighbor Count.....1
  Designated Router.....192.168.10.1
```


Command example:

If none of the interfaces are enabled for PIM, the following message is displayed:

```
None of the routing interfaces are enabled for PIM.
```

```
show ip pim neighbor
```

M4250

M4350

This command displays PIM neighbors discovered by PIMv2 Hello messages.

The interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

If the interface number is not specified, the command displays the status parameters of all PIM-enabled interfaces.

Format	<code>show ip pim neighbor [unit/slot/port vlan vlan-id]</code>
Modes	Privileged EXEC User EXEC
Term	Definition
Neighbor Address	The IP address of the PIM neighbor on an interface.
Interface	The interface number.
Up Time	The time since this neighbor has become active on this interface.
Expiry Time	Time remaining for the neighbor to expire.
DR Priority	The DR Priority configured on this Interface (PIM-SM only). Note: DR Priority is applicable only when sparse-mode configured routers are neighbors. Otherwise, NA is displayed in this field.

Command example:

```
(NETGEAR) #show ip pim neighbor 1/0/1
```

```
Neighbor Addr  Interface Uptime          Expiry Time DR
              (hh:mm:ss) (hh:mm:ss)  Priority
-----
192.168.10.2   1/0/1    00:02:55     00:01:15   NA
```

Command example:

```
(NETGEAR) #show ip pim neighbor
```

Neighbor Addr	Interface	Uptime (hh:mm:ss)	Expiry Time (hh:mm:ss)	DR Priority
192.168.10.2	1/0/1	00:02:55	00:01:15	1
192.168.20.2	1/0/2	00:03:50	00:02:10	1

Command example:

If no neighbors were learned on any of the interfaces, the following message is displayed:

```
No neighbors exist on the router.
```

```
show ip pim bsr-router
```

M4250

M4350

This command displays the bootstrap router (BSR) information.

Format	show ip pim bsr-router {candidate elected}
Mode	Privileged EXEC User EXEC

Parameter	Definition
BSR Address	IP address of the BSR.
BSR Priority	Priority as configured in the ip pim bsr-candidate command.
BSR Hash Mask Length	Length of a mask (maximum 32 bits) that is to be ANDed with the group address before the hash function is called. This value is configured in the ip pim bsr-candidate command.
C-BSR Advertisement Interval	Indicates the configured C-BSR Advertisement interval with which the router, acting as a C-BSR, will periodically send the C-BSR advertisement messages.
Next Bootstrap Message	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.

Command example:

```
(NETGEAR) #show ip pim bsr-router elected
```

```
BSR Address..... 192.168.10.1
BSR Priority..... 0
BSR Hash Mask Length..... 30
Next Bootstrap message (hh:mm:ss)..... 00:00:24
```

Command example:

```
(NETGEAR) #show ip pim bsr-router candidate
```

```
BSR Address..... 192.168.10.1
BSR Priority..... 0
BSR Hash Mask Length..... 30
C-BSR Advertisement Interval (secs)..... 60
Next Bootstrap message (hh:mm:ss)..... NA
```

Command example:

If no configured or elected BSRs exist on the router, the following message is displayed:

```
No BSR's exist/learned on this router.
```

show ip pim rp-hash

M4250

M4350

This command displays the rendezvous point (RP) selected for the specified group address.

Format	show ip pim rp-hash <i>group-address</i>

Modes	Privileged EXEC User EXEC

Term	Definition
RP Address	The IP address of the RP for the group specified.
Type	Indicates the mechanism (BSR or static) by which the RP was selected.

Command example:

```
(NETGEAR) #show ip pim rp-hash 224.1.2.0
```

```
RP Address 192.168.10.1
Type Static
```

Command example:

If no RP Group mapping exist on the router, the following message is displayed:

```
No RP-Group mappings exist/learned on this router.
```

show ip pim rp mapping

M4250

M4350

Use this command to display the mapping for the PIM group to the active Rendezvous points (RP) of which the router is aware (either configured or learned from the bootstrap router (BSR)). Use the optional parameters to limit the display to a specific RP address (*rp-address*) or to view group-to-candidate RP (**candidate**) or group to static RP mapping information (**static**).

Format	show ip pim rp mapping [<i>rp-address</i> candidate static]
Modes	Privileged EXEC User EXEC
Term	Definition
RP Address	The IP address of the RP for the group specified.
Group Address	The IP address of the multicast group.
Group Mask	The subnet mask associated with the group.
Origin	Indicates the mechanism (BSR or static) by which the RP was selected.
C-RP Advertisement Interval	Indicates the configured C-RP Advertisement interval with which the router acting as a Candidate RP will periodically send the C-RP advertisement messages to the elected BSR.

Command example:

```
(NETGEAR) #show ip pim rp mapping 192.168.10.1
RP Address      192.168.10.1
  Group Address 224.1.2.1
  Group Mask    255.255.255.0
  Origin        Static
```

Command example:

```
(NETGEAR) #show ip pim rp mapping

RP Address      192.168.10.1
  Group Address 224.1.2.1
  Group Mask    255.255.255.0
  Origin        Static

RP Address      192.168.20.1
  Group Address 229.2.0.0
  Group Mask    255.255.0.0
  Origin        Static
```

Command example:

```
(NETGEAR) # show ip pim rp mapping candidate

RP Address..... 192.168.10.1
Group Address..... 224.1.2.1
Group Mask..... 255.255.0.0
Origin..... BSR
C-RP Advertisement Interval (secs)..... 60
Next Candidate RP Advertisement (hh:mm:ss). 00:00:15
```

Command example:

If no RP Group mapping exist on the router, the following message is displayed:

```
No RP-Group mappings exist on this router.
```

show ip pim statistics

M4250

M4350

This command displays statistics for the received PIM control packets per interface. This command displays statistics only if PIM sparse mode is enabled.

The interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

Format	show ip pim statistics [<i>unit/slot/port</i> <i>vlan vlan-id</i>]

Modes	Privileged EXEC User EXEC

Term	Definition
Stat	• Rx packets received. • Tx packets transmitted.
Interface	The PIM-enabled routing interface.
Hello	The number of PIM Hello messages.
Register	The number of PIM Register messages.
Reg-Stop	The number of PIM Register-stop messages.

Term	Definition
Join/Pru	The number of PIM Join/Prune messages.
BSR	The number of PIM Boot Strap messages.
Assert	The number of PIM Assert messages.
CRP	The number of PIM Candidate RP Advertisement messages.

Command example:

```
(NETGEAR) #show ip pim statistics
=====
Interface  Stat   Hello Register Reg-Stop Join/Pru  BSR  Assert  CRP
=====
Vl10       Rx      0      0      0      0      0      0      0
           Tx      2      0      0      0      0      0      0

      Invalid Packets Received - 0
-----
Vl20       Rx      0      0      0      5      0      0      0
           Tx      8      7      0      0      0      0      0

      Invalid Packets Received - 0
-----
1/0/5      Rx      0      0      6      5      0      0      0
           Tx     10      9      0      0      0      0      0

      Invalid Packets Received - 0
-----
```

Command example:

```
(NETGEAR) #show ip pim statistics vlan 10
=====
Interface  Stat   Hello Register Reg-Stop Join/Pru  BSR  Assert  CRP
=====
Vl10       Rx      0      0      0      0      0      0      0
           Tx      2      0      0      0      0      0      0

      Invalid Packets Received - 0
-----
```

Command example:

```
(NETGEAR) #show ip pim statistics 1/0/5
=====
Interface  Stat    Hello Register Reg-Stop Join/Pru  BSR  Assert  CRP
=====
1/0/5      Rx       0         0         6         5      0       0       0
          Tx      10        9         0         0      0       0       0

Invalid Packets Received - 0
```

Internet Group Message Protocol Commands

This section describes the commands you use to view and configure Internet Group Message Protocol (IGMP) settings.

ip igmp

M4250

M4350

This command sets the administrative mode of IGMP in the system to active on an interface, range of interfaces, or on all interfaces.

Default	disabled
Format	ip igmp
Modes	Global Config Interface Config

no ip igmp

This command sets the administrative mode of IGMP in the system to inactive.

Format	no ip igmp
Modes	Global Config Interface Config

ip igmp header-validation

M4250

M4350

Use this command to enable header validation for IGMP messages.

Default	disabled
Format	ip igmp header-validation
Mode	Global Config

no ip igmp header-validation

This command disables header validation for IGMP messages.

Format	no ip igmp header-validation
Mode	Global Config

ip igmp version

M4250

M4350

This command configures the version of IGMP for an interface or range of interfaces. The version is either 1, 2 or 3.

Default	3
Format	ip igmp version {1 2 3}
Modes	Interface Config

no ip igmp version

This command resets the version of IGMP to the default value.

Format	no ip igmp version
Modes	Interface Config

ip igmp last-member-query-count

M4250

M4350

This command sets the number of Group-Specific Queries sent by the interface or range of interfaces before the router assumes that there are no local members on the interface. The range for *count* is from 1 to 20.

Format	<code>ip igmp last-member-query-count count</code>

Modes	Interface Config

no ip igmp last-member-query-count

This command resets the number of Group-Specific Queries to the default value.

Format	<code>no ip igmp last-member-query-count</code>

Modes	Interface Config

ip igmp last-member-query-interval

M4250

M4350

This command configures the Maximum Response Time inserted in Group-Specific Queries which are sent in response to Leave Group messages. The range for *deciseconds* is 0 to 255 tenths of a second. This value can be configured on one interface or a range of interfaces

Default	10 tenths of a second (1 second)

Format	<code>ip igmp last-member-query-interval deciseconds</code>

Modes	Interface Config

no ip igmp last-member-query-interval

This command resets the Maximum Response Time to the default value.

Format	<code>no ip igmp last-member-query-interval</code>

Modes	Interface Config

ip igmp query-interval

M4250

M4350

This command configures the query interval for the specified interface or range of interfaces. The query interval determines how fast IGMP Host-Query packets are transmitted on this interface. The range for the *seconds* argument is 1 to 3600 seconds.

Default	125 seconds
Format	<code>ip igmp query-interval seconds</code>
Modes	Interface Config

no ip igmp query-interval

This command resets the query interval for the specified interface to the default value. This is the frequency at which IGMP Host-Query packets are transmitted on this interface.

Format	<code>no ip igmp query-interval</code>
Modes	Interface Config

ip igmp query-max-response-time

M4250

M4350

This command configures the maximum response time interval for the specified interface or range of interfaces, which is the maximum query response time advertised in IGMPv2 queries on this interface. The *deciseconds* argument is the time interval, specified in 0 to 255 tenths of a second.

Default	100
Format	<code>ip igmp query-max-response-time deciseconds</code>
Mode	Interface Config

no ip igmp query-max-response-time

This command resets the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface to the default value. The maximum response time interval is reset to the default time.

Format	<code>no ip igmp query-max-response-time</code>
Mode	Interface Config

ip igmp robustness

M4250

M4350

This command configures the robustness that allows tuning of the interface or range of interfaces. The robustness is the tuning for the expected packet loss on a subnet. If a subnet is expected to have a lot of loss, the Robustness variable may be increased for the interface. The *number* argument specifies the packet loss number in the range from 1 to 255.

Default	2
Format	ip igmp robustness <i>number</i>
Mode	Interface Config

no ip igmp robustness

This command sets the robustness value to default.

Format	no ip igmp robustness
Mode	Interface Config

ip igmp startup-query-count

M4250

M4350

This command sets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface or range of interfaces. The range for the *number* argument is 1 to 20.

Default	2
Format	ip igmp startup-query-count <i>number</i>
Mode	Interface Config

no ip igmp startup-query-count

This command resets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface to the default value.

Format	no ip igmp startup-query-count
Mode	Interface Config

ip igmp startup-query-interval

M4250**M4350**

This command sets the interval between general queries sent on startup on the interface or range of interfaces. The time interval value is in seconds. The range for the *seconds* argument is 1 to 300 seconds.

Default	31
Format	<code>ip igmp startup-query-interval seconds</code>
Mode	Interface Config

no ip igmp startup-query-interval

This command resets the interval between general queries sent on startup on the interface to the default value.

Format	<code>no ip igmp startup-query-interval</code>
Mode	Interface Config

show ip igmp

M4250**M4350**

This command displays the system-wide IGMP information.

Format	<code>show ip igmp</code>
Modes	Privileged EXEC User EXEC

Term	Definition
IGMP Admin Mode	The administrative status of IGMP. This is a configured value.
Interface	The interface number.
Interface Mode	Indicates whether IGMP is enabled or disabled on the interface. This is a configured value.
Protocol State	The current state of IGMP on this interface. Possible values are Operational or Non-Operational.

show ip igmp groups

M4250

M4350

This command displays the registered multicast groups on the interface.

The interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

If **detail** is specified this command displays the registered multicast groups on the interface in detail.

Format	show ip igmp groups { <i>unit/slot/port</i> <i>vlan vlan-id</i> } [<i>detail</i>]
Mode	Privileged EXEC

If you do not use the **detail** keyword, the following fields display.

Term	Definition
IP Address	The IP address of the interface participating in the multicast group.
Subnet Mask	The subnet mask of the interface participating in the multicast group.
Interface Mode	This displays whether IGMP is enabled or disabled on this interface.

The following fields are not displayed if the interface is not enabled.

Term	Definition
Querier Status	This displays whether the interface has IGMP in Querier mode or Non-Querier mode.
Groups	The list of multicast groups that are registered on this interface.

If you use the **detail** keyword, the following fields display.

Term	Definition
Multicast IP Address	The IP address of the registered multicast group on this interface.
Last Reporter	The IP address of the source of the last membership report received for the specified multicast group address on this interface.
Up Time	The time elapsed since the entry was created for the specified multicast group address on this interface.

Term	Definition
Expiry Time	The amount of time remaining to remove this entry before it is aged out.
Version1 Host Timer	The time remaining until the local router assumes that there are no longer any IGMP version 1 multicast members on the IP subnet attached to this interface. This could be an integer value or "-----" if there is no Version 1 host present.
Version2 Host Timer	The time remaining until the local router assumes that there are no longer any IGMP version 2 multicast members on the IP subnet attached to this interface. This could be an integer value or "-----" if there is no Version 2 host present.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for this group on the specified interface.

show ip igmp interface

M4250

M4350

This command displays the IGMP information for an interface or VLAN.

The interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

Format	show ip igmp interface {unit/slot/port vlan vlan-id}
Modes	Privileged EXEC User EXEC

Term	Definition
Interface	The interface number.
IGMP Admin Mode	The administrative status of IGMP.
Interface Mode	Indicates whether IGMP is enabled or disabled on the interface.
IGMP Version	The version of IGMP running on the interface. This value can be configured to create a router capable of running either IGMP version 1 or 2.
Query Interval	The frequency at which IGMP Host-Query packets are transmitted on this interface.
Query Max Response Time	The maximum query response time advertised in IGMPv2 queries on this interface.
Robustness	The tuning for the expected packet loss on a subnet. If a subnet is expected to have a lot of loss, the Robustness variable may be increased for that interface.

Term	Definition
Startup Query Interval	The interval between General Queries sent by a Querier on startup.
Startup Query Count	The number of Queries sent out on startup, separated by the Startup Query Interval.
Last Member Query Interval	The Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages.
Last Member Query Count	The number of Group-Specific Queries sent before the router assumes that there are no local members.

show ip igmp interface membership

M4250

M4350

This command displays the list of interfaces that registered in the multicast group. The *multi-ipaddr* argument specifies the IP address of the multicast group.

Format `show ip igmp interface membership multi-ipaddr [detail]`

Mode Privileged EXEC

Term	Definition
Interface	The interface number.
Interface IP	The IP address of the interface participating in the multicast group.
State	The interface that has IGMP in Querier mode or Non-Querier mode.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for the specified group on this interface.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group on this interface. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

If you use the **detail** keyword, the following fields display.

Term	Definition
Interface	Valid unit and port number separated by a forward slash.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for the specified group on this interface.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group on this interface. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

Term	Definition
Source Hosts	The list of unicast source IP addresses in the group record of the IGMPv3 Membership Report with the specified multicast group IP address. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.
Expiry Time	The amount of time remaining to remove this entry before it is aged out. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

show ip igmp interface stats

M4250

M4350

This command displays the IGMP statistical information for the interface. The statistics are only displayed when the interface is enabled for IGMP.

The interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

Format	show ip igmp interface stats [<i>unit/slot/port</i> <i>vlan vlan-id</i>]
Modes	Privileged EXEC User EXEC

Term	Definition
Querier Status	The status of the IGMP router, whether it is running in Querier mode or Non-Querier mode.
Querier IP Address	The IP address of the IGMP Querier on the IP subnet to which this interface is attached.
Querier Up Time	The time since the interface Querier was last changed.
Querier Expiry Time	The amount of time remaining before the Other Querier Present Timer expires. If the local system is the querier, the value of this object is zero.
Wrong Version Queries	The number of queries received whose IGMP version does not match the IGMP version of the interface.
Number of Joins	The number of times a group membership has been added on this interface.
Number of Groups	The current number of membership entries for this interface.

IGMP Proxy Commands

The IGMP Proxy is used by IGMP Router (IPv4 system) to enable the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP router interfaces. With IGMP Proxy enabled, the system acts as proxy to all the hosts residing on its router interfaces.

`ip igmp-proxy`

M4250

M4350

This command enables the IGMP Proxy on the an interface or range of interfaces. To enable the IGMP Proxy on an interface, you must enable multicast forwarding. Also, be sure that there are no multicast routing protocols enabled on the switch.

Format	<code>ip igmp-proxy</code>
Mode	Interface Config

`no ip igmp-proxy`

This command disables the IGMP Proxy on the interface.

Format	<code>no ip igmp-proxy</code>
Mode	Interface Config

`ip igmp-proxy unsolicit-rprt-interval`

M4250

M4350

This command sets the unsolicited report interval for the IGMP Proxy interface or range of interfaces. This command is valid only when you enable IGMP Proxy on the interface or range of interfaces. The value for the *seconds* argument is a number in the range 1–260 seconds.

Default	1
Format	<code>ip igmp-proxy unsolicit-rprt-interval seconds</code>
Mode	Interface Config

no ip igmp-proxy unsolicit-rprt-interval

This command resets the unsolicited report interval of the IGMP Proxy router to the default value.

Format	no ip igmp-proxy unsolicit-rprt-interval

Mode	Interface Config

ip igmp-proxy reset-status

M4250

M4350

This command resets the host interface status parameters of the IGMP Proxy interface (or range of interfaces). This command is valid only when you enable IGMP Proxy on the interface.

Format	ip igmp-proxy reset-status

Mode	Interface Config

show ip igmp-proxy

M4250

M4350

This command displays a summary of the host interface status parameters. It displays the following parameters only when you enable IGMP Proxy.

Format	show ip igmp-proxy

Modes	Privileged EXEC User EXEC

Term	Definition
Interface index	The interface number of the IGMP Proxy.
Admin Mode	States whether the IGMP Proxy is enabled or not. This is a configured value.
Operational Mode	States whether the IGMP Proxy is operationally enabled or not. This is a status parameter.
Version	The present IGMP host version that is operational on the proxy interface.
Number of Multicast Groups	The number of multicast groups that are associated with the IGMP Proxy interface.
Unsolicited Report Interval	The time interval at which the IGMP Proxy interface sends unsolicited group membership report.

Term	Definition
Querier IP Address on Proxy Interface	The IP address of the Querier, if any, in the network attached to the upstream interface (IGMP-Proxy interface).
Older Version 1 Querier Timeout	The interval used to timeout the older version 1 queriers.
Older Version 2 Querier Timeout	The interval used to timeout the older version 2 queriers.
Proxy Start Frequency	The number of times the IGMP Proxy has been stopped and started.

Command example:

```
(NETGEAR Switch) #show ip igmp-proxy
```

```
Interface Index..... 1/0/1
Admin Mode..... Enable
Operational Mode..... Enable
Version..... 3
Num of Multicast Groups..... 0
Unsolicited Report Interval..... 1
Querier IP Address on Proxy Interface..... 5.5.5.50
Older Version 1 Querier Timeout..... 0
Older Version 2 Querier Timeout..... 00::00:00
Proxy Start Frequency..... 1
```

show ip igmp-proxy interface**M4250****M4350**

This command displays a detailed list of the host interface status parameters. It displays the following parameters only when you enable IGMP Proxy.

Format	show ip igmp-proxy interface
Modes	Privileged EXEC User EXEC

Term	Definition
Interface Index	The interface number of the IGMP proxy.

The column headings of the table associated with the interface are as follows.

Term	Definition
Ver	The IGMP version.
Query Rcvd	Number of IGMP queries received.
Report Rcvd	Number of IGMP reports received.
Report Sent	Number of IGMP reports sent.
Leaves Rcvd	Number of IGMP leaves received. Valid for version 2 only.
Leaves Sent	Number of IGMP leaves sent on the Proxy interface. Valid for version 2 only.

Command example:

```
(NETGEAR Switch) #show ip igmp-proxy interface
```

```
Interface Index..... 1/0/1
```

```
Ver  Query Rcvd  Report Rcvd  Report Sent  Leave Rcvd  Leave Sent
-----
1      0         0         0
2      0         0         0         0         0
3      0         0         0
```

show ip igmp-proxy groups

M4250

M4350

This command displays information about the subscribed multicast groups that IGMP Proxy reported. It displays a table of entries with the following as the fields of each column.

Format	show ip igmp-proxy groups
Modes	Privileged EXEC User EXEC

Term	Definition
Interface	The interface number of the IGMP Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of host that last sent a membership report for the current group on the network attached to the IGMP Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed since last created.

Term	Definition
Member State	The status of the entry. Possible values are IDLE_MEMBER or DELAY_MEMBER. - IDLE_MEMBER - interface has responded to the latest group membership query for this group. - DELAY_MEMBER - interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are Include or Exclude.
Sources	The number of sources attached to the multicast group.

Command example:

```
(NETGEAR Switch) #show ip igmp-proxy groups
Interface Index..... 1/0/1
Group Address      Last Reporter      Up Time      Member State  Filter Mode  Sources
-----
225.4.4.4          5.5.5.48          00:02:21     DELAY_MEMBER  Include      3
226.4.4.4          5.5.5.48          00:02:21     DELAY_MEMBER  Include      3
227.4.4.4          5.5.5.48          00:02:21     DELAY_MEMBER  Exclude      0
228.4.4.4          5.5.5.48          00:02:21     DELAY_MEMBER  Include      3
```

show ip igmp-proxy groups detail

M4250**M4350**

This command displays complete information about multicast groups that IGMP Proxy reported. It displays a table of entries with the following as the fields of each column.

Format	show ip igmp-proxy groups detail
Modes	Privileged EXEC User EXEC

Term	Definition
Interface	The interface number of the IGMP Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of host that last sent a membership report for the current group, on the network attached to the IGMP-Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed since last created.
Member State	The status of the entry. Possible values are IDLE_MEMBER or DELAY_MEMBER. - IDLE_MEMBER - interface has responded to the latest group membership query for this group. - DELAY_MEMBER - interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are Include or Exclude.
Sources	The number of sources attached to the multicast group.

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Group Source List	The list of IP addresses of the sources attached to the multicast group.
Expiry Time	Time left before a source is deleted.

Command example:

```
(NETGEAR Switch) #show ip igmp-proxy groups
```

```
Interface Index..... 1/0/1
```

Group Address	Last Reporter	Up Time	Member State	Filter Mode	Sources
225.4.4.4	5.5.5.48	00:02:21	DELAY_MEMBER	Include	3

Group Source List	Expiry Time
5.1.2.3	00:02:21
6.1.2.3	00:02:21
7.1.2.3	00:02:21

226.4.4.4	5.5.5.48	00:02:21	DELAY_MEMBER	Include	3

Group Source List	Expiry Time
2.1.2.3	00:02:21
6.1.2.3	00:01:44
8.1.2.3	00:01:44

227.4.4.4	5.5.5.48	00:02:21	DELAY_MEMBER	Exclude	0
228.4.4.4	5.5.5.48	00:03:21	DELAY_MEMBER	Include	3

Group Source List	Expiry Time
9.1.2.3	00:03:21
6.1.2.3	00:03:21
7.1.2.3	00:03:21

13

IPv6 Multicast Commands

This chapter describes the IPv6 multicast commands.

The chapter contains the following sections:

- [IPv6 Multicast Forwarder](#)
- [IPv6 PIM Commands](#)
- [IPv6 MLD Commands](#)
- [IPv6 MLD-Proxy Commands](#)

Note: No specific command exists to enable multicast for IPv6. If you enable multicast with a global config command, multicast is enabled for both IPv4 and IPv6.

The commands in this chapter are in one of three functional groups:

- **Show commands.** Display switch settings, statistics, and other information.
- **Configuration commands.** Configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- **Clear commands.** Clear some or all of the settings to factory defaults.

IPv6 Multicast Forwarder

ipv6 mroute

M4250

M4350

This command configures an IPv6 multicast static route for a source IPv6 address. You must set the source IPv6 address and associated prefix length and you set the IP address of the next-hop router. You must also set the preference value (from 1 to 255) for the route.

The optional interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

Default	No MRoute is configured on the system.
Format	<code>ipv6 mroute source-address/prefixlength rpf-addr [unit/slot/port vlan vlan-id] preference</code>
Mode	Global Config

Parameter	Description
source-address	The IPv6 address of the multicast source network.
prefixlength	The IPv6 mask of the multicast data source.
rpf-ip-addr	The IP address of the RPF next-hop router toward the source.
slot/port or unit/slot/port or vlan-id	[Optional] Specify the interface if the RPF Address is a link-local address.
preference	The administrative distance for this Static MRoute, that is, the preference value. The range is 1 to 255.

no ipv6 mroute

This command removes the configured IPv6 multicast static route.

Format	<code>no ip mroute source-address/prefixlength</code>
Mode	Global Config

Note: There is no specific IP multicast enable for IPv6. Enabling of multicast at global config is common for both IPv4 and IPv6.

show ipv6 mroute

M4250

M4350

Use this command to show the mroute entries that are specific to IPv6. (This command is the IPv6 equivalent of the IPv4 **show ip mroute** command.)

Format	show ipv6 mroute [detail summary]

Modes	Privileged EXEC User EXEC

If you use the **detail** parameter, the command displays the following Multicast Route Table fields.

Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Expiry Time	The time of expiry of this entry in seconds.
Up Time	The time elapsed since the entry was created in seconds.
RPF Neighbor	The IP address of the RPF neighbor.
Flags	The flags associated with this entry.

If you use the **summary** parameter, the command displays the following fields.

Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which the entry was created.
Incoming Interface	The interface on which the packet for the source/group arrives.
Outgoing Interface List	The list of outgoing interfaces on which the packet is forwarded.

show ipv6 mroute group

M4250**M4350**

This command displays the multicast configuration settings specific to IPv6 such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast route table containing the specified group IPv6 address *group-address*.

Format	show ipv6 mroute group <i>group-address</i> {detail summary}
Modes	Privileged EXEC User EXEC
Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which this entry was created.
Incoming Interface	The interface on which the packet for this group arrives.
Outgoing Interface List	The list of outgoing interfaces on which this packet is forwarded.

show ipv6 mroute source

M4250**M4350**

This command displays the multicast configuration settings that are specific to IPv6 such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast route table for the specified source IPv6 address (*source-address*).

Format	show ipv6 mroute source <i>source-address</i> {detail summary}
Modes	Privileged EXEC User EXEC

If you use the **detail** keyword, the command displays the following column headings in the output table.

Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Expiry Time	The time of expiry of this entry in seconds.

Term	Definition
Up Time	The time elapsed since the entry was created in seconds.
RPF Neighbor	The IP address of the RPF neighbor.
Flags	The flags associated with this entry.

If you use the **summary** keyword, the command displays the following column headings in the output table.

Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which this entry was created.
Incoming Interface	The interface on which the packet for this source arrives.
Outgoing Interface List	The list of outgoing interfaces on which this packet is forwarded.

show ipv6 mroute static

M4250

M4350

Use the **show ipv6 mroute static** command in Privileged EXEC or User EXEC mode to display all the configured IPv6 multicast static routes.

Format	<code>show ipv6 mroute static [source-address]</code>
Modes	Privileged EXEC User EXEC

Parameter	Description
Source Address	IP address of the multicast source network.
Source Mask	The subnetwork mask pertaining to the source IP.
RPF Address	The IP address of the RPF next-hop router toward the source.
Interface	The interface that is used to reach the RPF next-hop. This is valid if the RPF address is a link-local address.
Preference	The administrative distance for this Static MRoute.

clear ipv6 mroute

M4250

M4350

This command deletes all or the specified IPv6 multicast route entries.

Note: This command clears only dynamic mroute entries. It does not clear static mroutes.

Format	<code>clear ipv6 mroute { * <i>group-address</i> [<i>source-address</i>] }</code>
Modes	Privileged EXEC
Parameter	Description
*	Deletes all IPv6 entries from the IPv6 multicast routing table.
group-address	IPv6 address of the multicast group.
source-address	The IPv6 address of a multicast source that is sending multicast traffic to the group.

The following example deletes all entries from the IPv6 multicast routing table:

```
(NETGEAR Switch) # clear ipv6 mroute *
```

Command example:

The following example deletes all entries from the IPv6 multicast routing table that match the multicast group address (FF4E::1), irrespective of which source is sending for this group:

```
(NETGEAR Switch) # clear ipv6 mroute FF4E::1
```

Command example:

The following example deletes all entries from the IPv6 multicast routing table that match the multicast group address (FF4E::1) and the multicast source address (2001::2):

```
(NETGEAR Switch) # clear ipv6 mroute FF4E::1 2001::2
```

IPv6 PIM Commands

This section describes the commands you use to configure Protocol Independent Multicast -Dense Mode (PIM-DM) and Protocol Independent Multicast - Sparse Mode (PIM-SM) for IPv6 multicast routing. PIM-DM and PIM-SM are multicast routing protocols that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol. Only one PIM mode can be operational at a time.

ipv6 pim dense

M4250

M4350

This command enables the administrative mode of PIM-DM in the router.

Default	disabled
Format	ipv6 pim dense
Mode	Global Config

Command example:

```
(NETGEAR) (Config) #ipv6 pim dense
```

no ipv6 pim dense

This command disables the administrative mode of PIM-DM in the router.

Format	no ipv6 pim dense
Mode	Global Config

ipv6 pim sparse

M4250

M4350

This command enables the administrative mode of PIM-SM in the router.

Default	disabled
Format	ipv6 pim sparse
Mode	Global Config

Command example:

```
(NETGEAR) (Config) #ipv6 pim sparse
```

```
no ipv6 pim sparse
```

This command disables the administrative mode of PIM-SM in the router.

Format	no ipv6 pim sparse

Mode	Global Config

```
ipv6 pim
```

M4250

M4350

This command administratively enables PIM on an interface or range of interfaces.

Default	disabled

Format	ipv6 pim

Mode	Interface Config

Command example:

```
(NETGEAR) (Interface 1/0/1) #ipv6 pim
```

```
no ipv6 pim
```

This command sets the administrative mode of PIM on an interface to disabled.

Format	no ipv6 pim

Mode	Interface Config

```
ipv6 pim hello-interval
```

M4250

M4350

Use this command to configure the PIM hello interval for the specified router interface or range of interfaces. The *seconds* argument is the hello-interval, specified in the range 0–18000 seconds.

Default	30
Format	<code>ipv6 pim hello-interval <i>seconds</i></code>
Mode	Interface Config

Command example:

```
(NETGEAR) (Interface 1/0/1) #ipv6 pim hello-interval 50
```

```
no ipv6 pim hello-interval
```

Use this command to set the PIM hello interval to the default value.

Format	<code>no ipv6 pim hello-interval</code>
Mode	Interface Config

```
ipv6 pim bsr-border
```

M4250

M4350

Use this command to prevent bootstrap router (BSR) messages from being sent or received on the specified interface.

Note: This command takes effect only when PIM-SM is enabled in the Global mode.

Default	disabled
Format	<code>ipv6 pim bsr-border</code>
Mode	Interface Config

```
(NETGEAR) (Interface 1/0/1) #ipv6 pim bsr-border
```

```
no ipv6 pim bsr-border
```

Use this command to disable the setting of BSR border on the specified interface.

Format	<code>no ipv6 pim bsr-border</code>
Mode	Interface Config

ipv6 pim bsr-candidate

M4250**M4350**

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR).

The interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default	Disabled
Format	<code>ipv6 pim bsr-candidate interface {unit/slot/port vlan vlan-id} hash-mask-length [bsr-priority] [interval interval]</code>
Mode	Global Config
Parameters	Description
slot/port or unit/slot/port or vlan-id	The interface or VLAN number on this switch from which the BSR address is derived, to make it a candidate. This interface or VLAN must be enabled with PIM.
hash-mask-length	Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value was 24, only the first 24 bits of the group addresses matter. This allows you to get one RP for multiple groups.
bsr-priority	[Optional] Priority of the candidate BSR. The range is an integer from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IPv6 address is the BSR. The default value is 0.
interval	[Optional] Indicates the BSR candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.

Command example:

```
(NETGEAR) (Config) #ipv6 pim bsr-candidate interface 1/0/1 32 5
(NETGEAR) (Config) #ipv6 pim bsr-candidate interface 1/0/1 32 5 interval 100
```


no ipv6 pim bsr-candidate

This command is used to remove the configured PIM Candidate BSR router.

Format	no ipv6 pim bsr-candidate interface { <i>unit/slot/port</i> <i>vlan vlan-id</i> }

Mode	Global Config

ipv6 pim dr-priority

M4250

M4350

Use this command to set the priority value for which a router is elected as the designated router (DR). The *priority* argument is a value in the range of 0–2147483647.

Note: This command takes effect only when PIM-SM is enabled in the Global mode.

Default	1

Format	ipv6 pim dr-priority <i>priority</i>

Mode	Interface Config

Command example:

```
(NETGEAR) (Interface 1/0/1) #ipv6 pim dr-priority 10
```

no ipv6 pim dr-priority

Use this command to return the DR Priority on the specified interface to its default value.

Format	no ipv6 pim dr-priority

Mode	Interface Config

ipv6 pim join-prune-interval

M4250

M4350

This command is used to configure the join/prune interval for the PIM-SM router on an interface or range of interfaces. The join/prune interval is specified in seconds. The *seconds* argument can be configured as a value from 0 to 18000 seconds.

Note: This command takes effect only when PIM-SM is enabled in the Global mode.

Default	60
Format	<code>ipv6 pim join-prune-interval <i>seconds</i></code>
Mode	Interface Config

Command example: The following shows examples of the command.

```
(NETGEAR) (Interface 1/0/1) #ipv6 pim join-prune-interval 90
```

`no ipv6 pim join-prune-interval`

Use this command to set the join/prune interval on the specified interface to the default value.

Format	<code>no ipv6 pim join-prune-interval</code>
Mode	Interface Config

`ipv6 pim rp-address`

M4250

M4350

This command defines the address of a PIM Rendezvous point (RP) for a specific multicast group range.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default	0
Format	<code>ipv6 pim rp-address <i>rp-address</i> {<i>group-address/prefix-length</i> <i>prefix-list list-name</i>} [<i>override</i>]</code>
Mode	Global Config

Parameter	Description
<code>rp-address</code>	The IPv6 address of the RP.
<code>group-address/prefix-length</code>	The group address and prefix length supported by the RP.

Parameter	Description
list-name	The name of a list that contains group ranges for the RP.
override	[Optional] Indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

no ipv6 pim rp-address

This command is used to remove the address of the configured PIM Rendezvous point (RP) for the specified multicast group range.

Format	no ipv6 pim rp-address <i>rp-address</i> { <i>group-address/prefix-length</i> <i>prefix-list list-name</i> }
Mode	Global Config

ipv6 pim rp-candidate

M4250

M4350

This command is used to configure the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR) for a specific multicast group range.

The interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default	Disabled
Format	ipv6 pim rp-candidate interface { <i>unit/slot/port</i> <i>vlan vlan-id</i> } <i>group-address/prefixlength</i> [<i>interval interval</i>] [<i>priority value</i>]
Mode	Global Config

Parameter	Description
slot/port or unit/slot/port or vlan-id	The interface or VLAN ID is advertised as a candidate RP address. This interface or VLAN must be enabled with PIM.
group-address	The multicast group address that is advertised in association with the RP address.
prefixlength	The multicast group prefix that is advertised in association with the RP address.
interval	[Optional] Indicates the RP candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.
value	[Optional] Indicates the RP candidate advertisement priority value. The range is from 0 to 255.

no ipv6 pim rp-candidate

This command is used to disable the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Format no ipv6 pim rp-candidate interface {unit/slot/port | vlan vlan-id} group-address/prefixlength

Mode Global Config

ipv6 pim ssm

M4250

M4350

Use this command to define the Source Specific Multicast (SSM) range of IPv6 multicast addresses on the router.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Note: Some platforms do not support a non-zero data threshold rate. For these platforms, only a “Switch on First Packet” policy is supported.

Default disabled

Format ipv6 pim ssm {default | group-address/prefixlength}

Mode Global Config

Parameter	Description
default	Defines the SSM range access list FF3x::/32.

no ipv6 pim ssm

Use this command to remove the Source Specific Multicast (SSM) range of IP multicast addresses on the router.

Format	no ipv6 pim ssm {default <i>group-address/prefixlength</i> }

Mode	Global Config

clear ipv6 pim statistics

M4250

M4350

This commands clears all the IPv6 PIM statistics.

Format	clear ipv6 pim statistics

Modes	Privileged EXEC

show ipv6 pim

M4250

M4350

This command displays the system-wide information for PIM-DM or PIM-SM.

Format	show ipv6 pim

Modes	Privileged EXEC User EXEC

Note: If the PIM mode is PIM-DM (dense), some of the fields in the following table do not display in the command output because they are applicable only to PIM-SM.

Term	Definition
PIM Mode	Indicates whether the PIM mode is dense (PIM-DM) or sparse (PIM-SM)
Interface	<i>unit/slot/port</i>
Interface Mode	Indicates whether PIM is enabled or disabled on this interface.
Operational Status	The current state of PIM on this interface: Operational or Non-Operational.

The following example displays PIM Mode - Dense:

```
(NETGEAR) #show ipv6 pim
```

```
PIM Mode Dense
```

Interface	Interface-Mode	Operational-Status
-----	-----	-----
1/0/1	Enabled	Operational
1/0/3	Disabled	Non-Operational

Command example:

The following example displays PIM Mode - Sparse:

```
(NETGEAR) #show ipv6 pim
```

```
PIM Mode Sparse
```

Interface	Interface-Mode	Operational-Status
-----	-----	-----
1/0/1	Enabled	Operational
1/0/3	Disabled	Non-Operational

Command example:

The following example shows that PIM is not configured:

```
(NETGEAR) #show ipv6 pim
```

```
PIM Mode None
```

None of the routing interfaces are enabled for PIM.

show ipv6 pim ssm

M4250

M4350

This command displays the configured source specific IPv6 multicast addresses. If no SSM Group range is configured, the command output show the following message:

No SSM address range is configured.

Format	show ipv6 pim ssm
Modes	Privileged EXEC User EXEC

Term	Definition
Group Address	The IPv6 multicast address of the SSM group.
Prefix Length	The network prefix length.

show ipv6 pim interface

M4250

M4350

This command displays the interface information for PIM on the specified interface.

The interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

If no interface is specified, the command displays the status parameters for all PIM-enabled interfaces.

Format	show ipv6 pim interface [<i>unit/slot/port</i> <i>vlan vlan-id</i>]
Modes	Privileged EXEC User EXEC

Term	Definition
Interface	The interface number.
Mode	Indicates whether the PIM mode enabled on the interface is dense or sparse.
Hello Interval	The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.
Join Prune Interval	The join/prune interval for the PIM router. The interval is in seconds.
DR Priority	The priority of the Designated Router configured on the interface. This field is not applicable if the interface mode is Dense
BSR Border	Identifies whether this interface is configured as a bootstrap router border interface.
Neighbor Count	The number of PIM neighbors learned on this interface. This is a dynamic value and is shown only when a PIM interface is operational.
Designated Router	The IP address of the elected Designated Router for this interface. This is a dynamic value and will only be shown when a PIM interface is operational. This field is not applicable if the interface mode is Dense

Command example:

```
(NETGEAR) #show ipv6 pim interface
```

```
Interface.....1/0/1
  Mode.....Sparse
  Hello Interval (secs).....30
  Join Prune Interval (secs).....60
  DR Priority.....1
  BSR Border.....Disabled
  Neighbor Count.....1
  Designated Router.....192.168.10.1

Interface.....1/0/2
  Mode.....Sparse
  Hello Interval (secs).....30
  Join Prune Interval (secs).....60
  DR Priority.....1
  BSR Border.....Disabled
  Neighbor Count.....1
  Designated Router.....192.168.10.1
```

Command example:

If none of the interfaces are enabled for PIM, the following message is displayed:

```
None of the routing interfaces are enabled for PIM.
```

show ipv6 pim neighbor

M4250

M4350

This command displays PIM neighbors discovered by PIMv2 Hello messages.

The interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

If the interface number is not specified, this command displays the neighbors discovered on all the PIM-enabled interfaces.

Fully Managed Switches M4250 and M4350 Series

Format	<code>show ipv6 pim neighbor [unit/slot/port vlan vlan-id]</code>

Modes	Privileged EXEC User EXEC

Term	Definition
Neighbor Address	The IPv6 address of the PIM neighbor on an interface.
Interface	The interface number.
Up Time	The time since this neighbor has become active on this interface.
Expiry Time	Time remaining for the neighbor to expire.
DR Priority	The DR Priority configured on this Interface (PIM-SM only). Note: DR Priority is applicable only when sparse-mode configured routers are neighbors. Otherwise, NA is displayed in this field.

Command example:

```
(NETGEAR) #show ipv6 pim neighbor
```

Neighbor Addr	Interface	Uptime (HH:MM::SS)	Expiry Time (HH:MM::SS)
2001:DB8:39::/32	1/0/1	00:02:55	00:01:15
2001:DB8:A3::/32	1/0/2	00:03:50	00:02:10

Command example:

If no neighbors were learned on any of the interfaces, the following message is displayed:

```
No neighbors are learnt on any interface.
```

`show ipv6 pim bsr-router`

M4250

M4350

This command displays the bootstrap router (BSR) information.

Format	<code>show ipv6 pim bsr-router {candidate elected}</code>

Mode	Privileged EXEC User EXEC

Term	Definition
BSR Address	IPv6 address of the BSR.
BSR Priority	Priority as configured in the <code>ipv6 pim bsr-candidate</code> command.
BSR Hash Mask Length	Length of a mask (maximum 32 bits) that is to be ANDed with the group address before the hash function is called. This value is configured in the <code>ipv6 pim bsr-candidate</code> command.
C-BSR Advertisement Interval	Indicates the configured C-BSR Advertisement interval with which the router, acting as a C-BSR, will periodically send the C-BSR advertisement messages.
Next Bootstrap Message	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.

Command example:

```
(NETGEAR) #show ipv6 pim bsr-router elected

BSR Address..... 192.168.10.1
  BSR Priority..... 0
  BSR Hash Mask Length..... 30
  Next Bootstrap message (hh:mm:ss)..... 00:00:24
```

Command example:

```
(NETGEAR) #show ipv6 pim bsr-router candidate

BSR Address..... 192.168.10.1
  BSR Priority..... 0
  BSR Hash Mask Length..... 30
  C-BSR Advertisement Interval (secs)..... 60
  Next Bootstrap message (hh:mm:ss)..... NA
```

Command example:

If no configured or elected BSRs exist on the router, the following message is displayed:

```
No BSR's exist/learned on this router.
```

show ipv6 pim rp-hash

M4250

M4350

This command displays which rendezvous point (RP) is being used for a specified group that you must specify with the *group-address* argument.

Format	show ipv6 pim rp-hash <i>group-address</i>
Modes	Privileged EXEC User EXEC
Term	Definition
RP Address	The IPv6 address of the RP for the group specified.
Type	Indicates the mechanism (BSR or static) by which the RP was selected.

Command example:

```
(NETGEAR) #show ipv6 pim rp-hash 224.1.2.0
```

```
RP Address192.168.10.1
Type Static
```

Command example:

If no RP Group mapping exists on the router, the following message is displayed:

```
No RP-Group mappings exist/learned on this router.
```

show ipv6 pim rp mapping

M4250

M4350

Use this command to display the mapping for the PIM group to the active Rendezvous points (RP) of which the router is aware (either configured or learned from the bootstrap router [BSR]). Use the optional parameters to limit the display to a specific RP address (*rp-address*) or to view group-to-candidate RP (**candidate**) or group to Static RP mapping information (**static**).

Format	show ipv6 pim rp mapping [<i>rp-address</i> candidate static]
Modes	Privileged EXEC User EXEC

Term	Definition
RP Address	The IPv6 address of the RP for the group specified.
Group Address	The IPv6 address and prefix length of the multicast group.
Origin	Indicates the mechanism (BSR or static) by which the RP was selected.
C-RP Advertisement Interval	Indicates the configured C-RP Advertisement interval with which the router acting as a Candidate RP will periodically send the C-RP advertisement messages to the elected BSR.

Command example:

```
(NETGEAR) #show ipv6 pim rp mapping 192.168.10.1
```

```
RP Address      192.168.10.1
  Group Address 224.1.2.1
  Group Mask    255.255.255.0
  Origin        Static
```

Command example:

```
(NETGEAR) #show ipv6 pim rp mapping
```

```
RP Address      192.168.10.1
  Group Address 224.1.2.1
  Group Mask    255.255.255.0
  Origin        Static
```

```
RP Address      192.168.20.1
  Group Address 229.2.0.0
  Group Mask    255.255.0.0
  Origin        Static
```

Command example:

```
(NETGEAR) # show ipv6 pim rp mapping candidate
```

```
RP Address..... 192.168.10.1
  Group Address..... 224.1.2.1
  Group Mask..... 255.255.0.0
  Origin..... BSR
  C-RP Advertisement Interval (secs)..... 60
  Next Candidate RP Advertisement (hh:mm:ss). 00:00:15
```

Command example:

If no RP Group mapping exist on the router, the following message is displayed:

```
No RP-Group mappings exist on this router.
```

show ipv6 pim statistics

M4250

M4350

This command displays statistics for the received PIM control packets per interface. This command displays statistics only if PIM sparse mode is enabled.

The interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

Format	show ipv6 pim statistics [<i>unit/slot/port</i> <i>vlan vlan-id</i>]
Modes	Privileged EXEC User EXEC

Term	Definition
Stat	• Rx packets received. • Tx packets transmitted.
Interface	The PIM-enabled routing interface.
Hello	The number of PIM Hello messages.
Register	The number of PIM Register messages.
Reg-Stop	The number of PIM Register-stop messages.
Join/Pru	The number of PIM Join/Prune messages.
BSR	The number of PIM Boot Strap messages.
Assert	The number of PIM Assert messages.
CRP	The number of PIM Candidate RP Advertisement messages.

Command example:

```
(NETGEAR) #show ipv6 pim statistics
=====
Interface  Stat   Hello Register Reg-Stop Join/Pru  BSR  Assert  CRP
=====
Vl10      Rx      0      0      0      0      0      0      0
          Tx      2      0      0      0      0      0      0

Invalid Packets Received - 0
```

```
-----
Vl10      Rx      0      0      0      5      0      0      0
          Tx      8      7      0      0      0      0      0
-----
```

Invalid Packets Received - 0

```
-----
1/0/5     Rx      0      0      6      5      0      0      0
          Tx     10      9      0      0      0      0      0
-----
```

Invalid Packets Received - 0

Command example:

```
(NETGEAR) #show ipv6 pim statistics vlan 10
```

```
=====
Interface  Stat   Hello Register Reg-Stop Join/Pru  BSR  Assert  CRP
=====
Vl10       Rx      0      0      0      0      0      0      0
          Tx      2      0      0      0      0      0      0
-----
```

Invalid Packets Received - 0

Command example:

```
(NETGEAR) #show ipv6 pim statistics 1/0/5
```

```
=====
Interface  Stat   Hello Register Reg-Stop Join/Pru  BSR  Assert  CRP
=====
1/0/5      Rx      0      0      6      5      0      0      0
          Tx     10      9      0      0      0      0      0
-----
```

Invalid Packets Received - 0

IPv6 MLD Commands

IGMP and MLD snooping are Layer 2 functionalities but IGMP and MLD are Layer 3 multicast protocols. If you want to use IGMP and MLD snooping, a network must include a multicast router that can function as a querier to solicit multicast group registrations. However, if multicast traffic is destined to hosts within the same network, a multicast router is not required but an IGMP and MLD snooping querier must be running on one of the switches in the network and snooping must be enabled on all switches in the network. For more information,

see [IGMP Snooping Configuration Commands on page 753](#) and [MLD Snooping Commands on page 777](#).

ipv6 mld router

M4250

M4350

Use this command, in the administrative mode of the router, to enable MLD in the router.

Default	Disabled
Format	ipv6 mld router
Mode	Global Config

no ipv6 mld router

Use this command, in the administrative mode of the router, to disable MLD in the router.

Default	Disabled
Format	no ipv6 mld router
Mode	Global Config

ipv6 mld query-interval

M4250

M4350

Use this command to set the MLD router's query interval for the interface or range of interfaces. The query-interval is the amount of time between the general queries sent when the router is the querier on that interface. The range for the *seconds* argument is from 1 to 3600 seconds.

Default	125
Format	ipv6 mld query-interval <i>seconds</i>
Mode	Interface Config

no ipv6 mld query-interval

Use this command to reset the MLD query interval to the default value for that interface.

Format	no ipv6 mld query-interval
Mode	Interface Config

ipv6 mld query-max-response-time

M4250

M4350

Use this command to set the MLD querier's maximum response time for the interface or range of interfaces and this value is used in assigning the maximum response time in the query messages that are sent on that interface. The range for the *milliseconds* argument is from 0 to 65535 milliseconds.

Default	10000 milliseconds
Format	ipv6 mld query-max-response-time <i>milliseconds</i>
Mode	Interface Config

no ipv6 mld query-max-response-time

This command resets the MLD query max response time for the interface to the default value.

Format	no ipv6 mld query-max-response-time
Mode	Interface Config

ipv6 mld startup-query-interval

M4250

M4350

Use this command to set the interval between general IPv6 MLD queries that are sent when the MLP process starts on the interface or range of interfaces. The range for the *seconds* argument is 1 to 300 seconds. The default is 31 seconds.

Default	31
Format	ipv6 mld startup-query-interval <i>seconds</i>
Mode	Interface Config

no ipv6 mld startup-query-interval

Use this command to reset the startup query interval for IPv6 MLD to the default value of 31 seconds.

Format	no ipv6 mld startup-query-interval
Mode	Interface Config

ipv6 mld startup-query-count

M4250

M4350

Use this command to specify the number of IPv6 MLD queries that are sent when the MLP process starts on the interface or range of interfaces and that is separated by the startup query interval on the interface or range of interfaces. The range for the *number* argument is 1 to 20. The default is 2.

Default	2
Format	<code>ipv6 mld startup-query-count <i>number</i></code>
Mode	Interface Config

no ipv6 mld startup-query-count

Use this command to reset the startup query count for IPv6 MLD to the default value of 2.

Format	<code>no ipv6 mld startup-query-count</code>
Mode	Interface Config

ipv6 mld last-member-query-interval

M4250

M4350

Use this command to set the last member query interval for an MLD interface or range of interfaces, which is the value of the maximum response time parameter in the group specific queries sent out of this interface. The range for the *milliseconds* argument is from 0 to 65535 milliseconds.

Default	1000 milliseconds
Format	<code>ipv6 mld last-member-query-interval <i>milliseconds</i></code>
Mode	Interface Config

no ipv6 mld last-member-query-interval

Use this command to reset the last member query interval of the interface to the default value.

Format	<code>no ipv6 mld last-member-query-interval</code>
Mode	Interface Config

ipv6 mld last-member-query-count

M4250

M4350

Use this command to set the number of listener-specific queries sent before the router assumes that there are no local members on an interface or range of interfaces. The range for the *number* argument is 1 to 20.

Default	2
Format	ipv6 mld last-member-query-count <i>number</i>
Mode	Interface Config

no ipv6 mld last-member-query-count

Use this command to reset the last member query count of the interface to the default value.

Format	no ipv6 mld last-member-query-count
Mode	Interface Config

ipv6 mld version

M4250

M4350

Use this command to configure the MLD version that the interface uses.

Default	2
Format	ipv6 mld version {1 2}
Mode	Interface Config

no ipv6 mld version

This command resets the MLD version used by the interface to the default value.

Format	no ipv6 mld
Mode	Interface Config

show ipv6 mld groups

M4250

M4350

Use this command to display information about multicast groups that MLD reported. The information is displayed only when MLD is enabled on at least one interface. If MLD was not enabled on even one interface, there is no group information to be displayed.

The interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

You can also specify a group address (*group-address*).

Format	<code>show ipv6 mld groups {unit/slot/port vlan vlan-id group-address}</code>
Mode	Privileged EXEC User EXEC

The following fields are displayed as a table when you specify an interface.

Field	Description
Group Address	The address of the multicast group.
Interface	Interface through which the multicast group is reachable.
Up Time	Time elapsed in hours, minutes, and seconds since the multicast group has been known.
Expiry Time	Time left in hours, minutes, and seconds before the entry is removed from the MLD membership table.

When *group-address* is specified, the following fields are displayed for each multicast group and each interface.

Field	Description
Interface	Interface through which the multicast group is reachable.
Group Address	The address of the multicast group.
Last Reporter	The IP Address of the source of the last membership report received for this multicast group address on that interface.
Filter Mode	The filter mode of the multicast group on this interface. The values it can take are include and exclude.

Field	Description
Version 1 Host Timer	The time remaining until the router assumes there are no longer any MLD version-1 Hosts on the specified interface.
Group Compat Mode	The compatibility mode of the multicast group on this interface. The values it can take are MLDv1 and MLDv2.

The following table is displayed to indicate all the sources associated with this group.

Field	Description
Source Address	The IP address of the source.
Uptime	Time elapsed in hours, minutes, and seconds since the source has been known.
Expiry Time	Time left in hours, minutes, and seconds before the entry is removed.

Command example:

```
(NETGEAR Switch) #show ipv6 mld groups ?
```

```
group-address          Enter Group Address Info.
<unit/port>           Enter interface in unit/port format.
```

Command example:

```
(NETGEAR Switch) #show ipv6 mld groups 1/0/1
```

```
Group Address..... FF43::3
Interface..... 1/0/1
Up Time (hh:mm:ss)..... 00:03:04
Expiry Time (hh:mm:ss)..... -----
```

Command example:

```
(NETGEAR Switch) #show ipv6 mld groups ff43::3
```

```
Interface..... 1/0/1
Group Address..... FF43::3
Last Reporter..... FE80::200:FF:FE00:3
Up Time (hh:mm:ss)..... 00:02:53
Expiry Time (hh:mm:ss)..... -----
Filter Mode..... Include
Version1 Host Timer..... -----
Group compat mode..... v2
Source Address      ExpiryTime
-----
2003::10            00:04:17
2003::20            00:04:17
```

show ipv6 mld interface

M4250

M4350

Use this command to display MLD-related information for all interfaces, a specific interface, or a VLAN.

The interface corresponds to a physical routing interface or VLAN routing interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

The **vlan** keyword and *vlan-id* parameter are used to specify the VLAN ID of the routing VLAN. The *vlan-id* parameter is a number in the range of 1–4093.

Format	show ipv6 mld interface {all unit/slot/port vlan vlan-id}
Mode	Privileged EXEC User EXEC

The following information is displayed for each of the interfaces or for only the specified interface.

Field	Description
Interface	The interface number.
MLD Mode	Displays the configured administrative status of MLD.
Operational Mode	The operational status of MLD on the interface.
MLD Version	Indicates the version of MLD configured on the interface.
Query Interval	Indicates the configured query interval for the interface.
Query Max Response Time	Indicates the configured maximum query response time (in seconds) advertised in MLD queries on this interface.
Robustness	Displays the configured value for the tuning for the expected packet loss on a subnet attached to the interface.
Startup Query interval	This value indicates the configured interval between General Queries sent by a Querier on startup.
Startup Query Count	This value indicates the configured number of Queries sent out on startup, separated by the Startup Query Interval.
Last Member Query Interval	This value indicates the configured Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages.
Last Member Query Count	This value indicates the configured number of Group-Specific Queries sent before the router assumes that there are no local members.

The following information is displayed if the operational mode of the MLD interface is enabled.

Field	Description
Querier Status	This value indicates whether the interface is an MLD querier or non-querier on the subnet it is associated with.
Querier Address	The IP address of the MLD querier on the subnet the interface is associated with.
Querier Up Time	Time elapsed in seconds since the querier state has been updated.
Querier Expiry Time	Time left in seconds before the Querier loses its title as querier.
Wrong Version Queries	Indicates the number of queries received whose MLD version does not match the MLD version of the interface.
Number of Joins	The number of times a group membership has been added on this interface.
Number of Leaves	The number of times a group membership has been removed on this interface.
Number of Groups	The current number of membership entries for this interface.

show ipv6 mld traffic

M4250

M4350

Use this command to display MLD statistical information for the router.

Format	show ipv6 mld traffic
Mode	Privileged EXEC User EXEC

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.
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.
Bad Checksum MLD Packets	The number of bad checksum MLD packets received by the router.
Malformed MLD Packets	The number of malformed MLD packets received by the router.

clear ipv6 mld counters

M4250

M4350

Use this command to reset the MLD counters to zero on the specified interface. The optional interface corresponds to a physical interface. To specify an actual interface or port, do the following:

- For an M4250 series switch, use the argument *slot/port*.
- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	clear ipv6 mld counters [<i>unit/slot/port</i>]
Mode	Privileged Exec

clear ipv6 mld traffic

M4250

M4350

Use this command to clear all entries in the MLD traffic database.

Format	clear ipv6 mld traffic
Mode	Privileged Exec

IPv6 MLD-Proxy Commands

MLD-Proxy is the IPv6 equivalent of IGMP-Proxy. MLD-Proxy commands allow you to configure the network device as well as to view device settings and statistics using either serial interface or telnet session. The operation of MLD-Proxy commands is the same as for IGMP-Proxy: MLD is for IPv6 and IGMP is for IPv4. MGMD is a term used to refer to both IGMP and MLD.

ipv6 mld-proxy

M4250

M4350

Use this command to enable MLD-Proxy on the interface or range of interfaces. To enable MLD-Proxy on the interface, you must enable multicast forwarding. Also, make sure that there are no other multicast routing protocols enabled on the router.

Format	<code>ipv6 mld-proxy</code>
Mode	Interface Config

no ipv6 mld-proxy

Use this command to disable MLD-Proxy on the router.

Format	<code>no ipv6 mld-proxy</code>
Mode	Interface Config

ipv6 mld-proxy unsolicit-rprt-interval

M4250

M4350

Use this command to set the unsolicited report interval for the MLD-Proxy interface or range of interfaces. This command is only valid when you enable MLD-Proxy on the interface. The value of *interval* is 1-260 seconds.

Default	1
Format	<code>ipv6 mld-proxy unsolicit-rprt-interval interval</code>
Mode	Interface Config

no ipv6 mld-proxy unsolicited-report-interval

Use this command to reset the MLD-Proxy router's unsolicited report interval to the default value.

Format	<code>no ipv6 mld-proxy unsolicit-rprt-interval</code>
Mode	Interface Config

ipv6 mld-proxy reset-status

M4250**M4350**

Use this command to reset the host interface status parameters of the MLD-Proxy interface or range of interfaces. This command is only valid when you enable MLD-Proxy on the interface.

Format	ipv6 mld-proxy reset-status

Mode	Interface Config

show ipv6 mld-proxy

M4250**M4350**

Use this command to display a summary of the host interface status parameters.

Format	show ipv6 mld-proxy

Mode	Privileged EXEC User EXEC

The command displays the following parameters only when you enable MLD-Proxy.

Field	Description
Interface Index	The interface number of the MLD-Proxy.
Admin Mode	Indicates whether MLD-Proxy is enabled or disabled. This is a configured value.
Operational Mode	Indicates whether MLD-Proxy is operationally enabled or disabled. This is a status parameter.
Version	The present MLD host version that is operational on the proxy interface.
Number of Multicast Groups	The number of multicast groups that are associated with the MLD-Proxy interface.
Unsolicited Report Interval	The time interval at which the MLD-Proxy interface sends unsolicited group membership report.
Querier IP Address on Proxy Interface	The IP address of the Querier, if any, in the network attached to the upstream interface (MLD-Proxy interface).
Older Version 1 Querier Timeout	The interval used to timeout the older version 1 queriers.
Proxy Start Frequency	The number of times the MLD-Proxy has been stopped and started.

Command example:

```
(NETGEAR Switch) #show ipv6 mld-proxy
Interface Index..... 1/0/3
Admin Mode..... Enable
```

```

Operational Mode..... Enable
Version..... 3
Num of Multicast Groups..... 0
Unsolicited Report Interval..... 1
Querier IP Address on Proxy Interface..... fe80::1:2:5
Older Version 1 Querier Timeout..... 00:00:00
Proxy Start Frequency.....

```

show ipv6 mld-proxy interface

M4250

M4350

This command displays a detailed list of the host interface status parameters. It displays the following parameters only when you enable MLD-Proxy.

Format	show ipv6 mld-proxy interface
Modes	Privileged EXEC User EXEC

Term	Definition
Interface Index	The interface for the MLD-proxy.

The column headings of the table associated with the interface are as follows.

Term	Definition
Ver	The MLD version.
Query Rcvd	Number of MLD queries received.
Report Rcvd	Number of MLD reports received.
Report Sent	Number of MLD reports sent.
Leaves Rcvd	Number of MLD leaves received. Valid for version 2 only.
Leaves Sent	Number of MLD leaves sent on the Proxy interface. Valid for version 2 only.

Command example:

```

(NETGEAR Switch) #show ipv6 mld-proxy interface
Interface Index..... 1/0/1

```

```

Ver  Query Rcvd  Report Rcvd  Report Sent  Leave Rcvd  Leave Sent
-----
1      2          0          0          0          2
2      3          0          4

```

show ipv6 mld-proxy groups

M4250

M4350

Use this command to display information about multicast groups that the MLD-Proxy reported.

Format	show ipv6 mld-proxy groups
Mode	Privileged EXEC User EXEC
Field	Description
Interface	The interface number of the MLD-Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of the host that last sent a membership report for the current group, on the network attached to the MLD-Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed in seconds since last created.
Member State	Possible values are: - Idle_Member. The interface has responded to the latest group membership query for this group. - Delay_Member. The interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are Include or Exclude.
Sources	The number of sources attached to the multicast group.

Command example:

```
(NETGEAR Switch) #show ipv6 mld-proxy groups
```

```
Interface Index..... 1/0/3
Group Address    Last Reporter    Up Time    Member State    Filter Mode    Sources
-----
FF1E::1         FE80::100:2.3    00:01:40    DELAY_MEMBER    Exclude        2
FF1E::2         FE80::100:2.3    00:02:40    DELAY_MEMBER    Include        1
FF1E::3         FE80::100:2.3    00:01:40    DELAY_MEMBER    Exclude        0
FF1E::4         FE80::100:2.3    00:02:44    DELAY_MEMBER    Include        4
```

show ipv6 mld-proxy groups detail

M4250**M4350**

Use this command to display information about multicast groups that MLD-Proxy reported.

Format	show ipv6 mld-proxy groups detail
Mode	Privileged EXEC User EXEC
Field	Description
Interface	The interface number of the MLD-Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of the host that last sent a membership report for the current group, on the network attached to the MLD-Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed in seconds since last created.
Member State	Possible values are: - Idle_Member. The interface has responded to the latest group membership query for this group. - Delay_Member. The interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values
Sources	The number of sources attached to the multicast group. are Include or Exclude.
Group Source List	The list of IP addresses of the sources attached to the multicast group.
Expiry Time	The time left for a source to get deleted.

Command example:

```
(NETGEAR Switch) #show ipv6 igmp-proxy groups
```

```
Interface Index..... 1/0/3
```

Group Address	Last Reporter	Up Time	Member State	Filter Mode	Sources
-----	-----	-----	-----	-----	-----
FF1E::1	FE80::100:2.3	244	DELAY_MEMBER	Exclude	2
Group Source List		Expiry Time			
-----		-----			
2001::1		00:02:40			
2001::2					
FF1E::2	FE80::100:2.3	243	DELAY_MEMBER	Include	1

Fully Managed Switches M4250 and M4350 Series

Group	Source List	Expiry Time
-----		-----
	3001::1	00:03:32
	3002::2	00:03:32
FF1E::3	FE80::100:2.3	328
FF1E::4	FE80::100:2.3	255
	DELAY_MEMBER	Exclude
	DELAY_MEMBER	Include
		0
		4

Group	Source List	Expiry Time
-----		-----
	4001::1	00:03:40
	5002::2	00:03:40
	4001::2	00:03:40
	5002::2	00:03:40

14

Power over Ethernet Commands

This chapter contains the following sections:

- [About PoE](#)
- [PoE Commands](#)

About PoE

Power over Ethernet (PoE) describes a technology to pass electrical power safely along with data on existing Ethernet cabling. The power supply equipment (PSE) is the device or switch that delivers electrical power, and the PD or powered device is the end device that powers up through the power delivered along the Ethernet cable.

The switch supports PoE, PoE+, and PoE++:

- **PoE (802.3af)**. This is the original standard, also known as the low-power standard, which mandates delivery of up to 15.4 watts by the PSE. Because of power dissipation, only 12.95 watts are assured to be available at the powered device (PD). The PD needs to be designed so that it can accept power over Ethernet cabling. Category 3 cables can be used to deliver power to the PD. However, with the advent of 802.11n, the newer wireless APs required more power. To account for this, a newer standard was developed in 2009, known as 802.3at.
- **PoE+ (802.3at)**. This mode is also known as the high-power standard, which mandates delivery of up to 34.2 watts by the PSE. Because of power dissipation, PoE+ provides only a maximum of 25.5 watts at the powered device. Some PSEs can provide up to 51 watts. Before this standard became available in 2009, the industry started using different implementations to allow for more power. All these needed to be brought under the purview of the newer 802.3at standard.
- **PoE++ (802.3bt)**. This mode is also known as the ultra-power standard. On a M4350 series switch model that is capable of supporting 802.3bt, this is the default mode. The maximum PoE power supported by PoE++ is 96.5W.

Note: PoE, PoE+, and PoE++ are supported only on physical, copper interfaces. The default port mode depends on the M4350 series switch model.

PoE Commands

poe

M4250

M4350

Use this command to enable the Power over Ethernet (PoE) functionality on a global basis or per interface.

Default	enabled
Format	poe
Mode	Global Config Interface Config

no poe

Use this command to disable the Power over Ethernet (PoE) functionality on a global basis or per interface.

Format	no poe
Mode	Global Config Interface Config

poe detection

M4250

M4350

Use this command to configure the detection type on an interface. Use the command to configure which types of PDs are detected and powered by the switch.

Note: By default, a switch that supports PoE++ power starts in 802.3bt mode. By default, a switch that support PoE+ power starts up in 802.3at mode.

The switch supports the following three detection options:

- **4ptdot3af.** 4-point dot3af detection. The port performs a 4-point 802.3af resistive detection.
- **4ptdot3af+legacy.** The port performs a 4-point 802.3af resistive detection, and if required, continues with legacy detection.

- **legacy**. Legacy detection. The port is powered using high-inrush current, which is used by legacy PDs that require more than 15W to power up.

Default	4ptdot3af
Format	poe detection [4ptdot3af 4ptdot3af+legacy legacy]
Mode	Interface Config

no poe detection

Use this command to set the detection mode to the default on an interface.

Format	no poe detection
Mode	Interface Config

poe power limit user-defined

M4250

M4350

Use this command to configure the PoE power limit in mW on an interface.

The value of *power* can be from 3000 mW to the maximum supported limit in mW for the switch model.

Format	poe power limit user-defined [power]
Mode	Interface Config

poe high-power

M4250

M4350

Use this command to manually configure the high-power mode on an interface. This mode is used to power up devices that require more power than 802.3af power (more than 12.95 watts at the PD). These are the options:

- **dot3at**. The port is powered in the IEEE 802.3at mode and is backward compatible with IEEE 802.3af. In this mode, if the switch detects that the attached PD requests more power than IEEE 802.3af but is not an IEEE 802.3at Class 4 device, the PD does not receive power from the switch. This mode supports LLDP.
- **dot3bt**. The port is powered in the IEEE 802.3bt mode and is backward compatible with IEEE 802.3at and IEEE 802.3af. In this mode, if the switch detects that the attached PD requests more power than IEEE 802.3at but is not an IEEE 802.3bt device, the PD does not receive power from the switch. This mode supports LLDP.
- **dot3bt-type3**. The port supports the IEEE 802.3bt Type 3 mode, the IEEE 802.3at mode, and the IEEE 802.3af mode.

- **legacy**. The port is powered using high-inrush current, which is used by legacy PDs that require more than 15W to power up.
- **pre-dot3at**. The port is initially powered in the IEEE 802.3af mode and, before 75 msec pass, is switched to the high power IEEE 802.3at mode. Select this mode if the PD does not perform Layer 2 classification or if the switch performs 2-event Layer 1 classification. This mode does not support LLDP.
- **pre-dot3bt**. The port supports Class 4 devices that use 4-pair PoE (4PPoE) to receive power higher than 30W but that are not compliant with IEEE 802.3bt. The port also supports the IEEE 802.3at and IEEE 802.3af modes. This mode does not support LLDP.

For a switch the supports PoE++:

Default	dot3bt
Format	poe high-power [dot3at dot3bt dot3bt-type3 legacy pre-dot3at pre-dot3bt]
Mode	Interface Config

For a switch the supports PoE+:

Default	dot3at
Format	poe high-power [dot3at legacy pre-dot3at]
Mode	Interface Config

no poe high-power

Use this command to disable the high-power mode. The port support 802.3af devices only.

This command works on a per-interface basis.

Format	no poe high-power
Mode	Interface Config

poe power limit

M4250

M4350

Use this command to configure the type of power limit for a port. If the power limit type is **user-defined**, the command also allows you to configure a maximum power limit.

There are three options:

- **class-based**. Allows the port to draw up to the maximum power based on the classification of the device connected.
- **none**. Allows the port to draw up to Class 0 maximum power if it is in low-power mode and up to Class 4 maximum power if it is in high-power mode.

- **user-defined.** Allows you to define the maximum power to the port. This can be a value from 3 through 32 watts. Therefore, the range is 3000–32000 mW.

Default	Class-based
Format	<code>poe power limit {class-based none user-defined <i>maximum-power</i>}</code>
Mode	Global Config Interface Config

no poe power limit

Use this command to set the power limit type to the default. It also sets the maximum power limit to the default if the power limit type is user-defined.

Format	<code>no poe power limit [user-defined]</code>
Mode	Global Config Interface Config

poe power management (M4250 series switch)

M4250

Use this command to configure the power management mode based on each individual PoE unit or on all PoE units.

Both the power management modes mentioned here will power up a device based on first come, first served. When the available power is less than the power limit defined on a port, no more power will be delivered.

Static and dynamic modes differ in how the available power is calculated, as follows:

- Static Power Management

Available power = power limit of the source - total allocated power

Where total allocated power is calculated as the power limit configured on the port.

- Dynamic Power Management

Available power = power limit of the source - total allocated power

Where total allocated power is calculated as the amount of power consumed by the port.

For example:

Assume that the power limit of the source is 300 watts. One port is powered up and is drawing 3 watts of power. The power limit defined on the port is user-defined as 15 watts. In this case, the available power for static and dynamic would be as follows:

- Static Power Management

Available power = 300 watts - 15 watts = 285 watts

- Dynamic Power Management

Available power = 300 watts - 3 watts = 297 watts

Default	dynamic
Format	poe power management {dynamic static}
Mode	Global Config

no poe power management (M4250 series switch)

Use this command to set the power management mode to the default.

Format	no poe power management
Mode	Global Config

poe power management (M4350 series switch)

M4350

Use this command to configure the power management mode based on each individual PoE unit or on all PoE units.

Both the power management modes mentioned here will power up a device based on first come, first served. When the available power is less than the power limit defined on a port, no more power will be delivered.

Static and dynamic modes differ in how the available power is calculated, as follows:

- Static Power Management

Available power = power limit of the source - total allocated power

Where total allocated power is calculated as the power limit configured on the port.

- Dynamic Power Management

Available power = power limit of the source - total allocated power

Where total allocated power is calculated as the amount of power consumed by the port.

For example:

Assume that the power limit of the source is 300 watts. One port is powered up and is drawing 3 watts of power. The power limit defined on the port is user-defined as 15 watts. In this case, the available power for static and dynamic would be as follows:

- Static Power Management

Available power = 300 watts - 15 watts = 285 watts

- Dynamic Power Management

Available power = 300 watts - 3 watts = 297 watts

Default	dynamic
Format	poe power management {unit all} {dynamic static}
Mode	Global Config

no poe power management (M4350 series switch)

Use this command to set the power management mode to the default.

Format	no poe power management {unit all}
Mode	Global Config

poe priority

M4250

M4350

Use this command to configure the priority on a specific port. This is used for power management purposes. The switch might not be able to supply power to all connected devices, so the port priority is used to determine which ports will supply power if adequate power capacity is not available for all enabled ports. For ports that have the same priority level, the lower numbered port will have higher priority.

If a switch delivers peak power to a number of devices and you attach a new device to a high-priority port, the switch can shut down power to a low-priority port before it powers up the new device.

Default	low
Format	poe priority [crit high low medium]
Mode	Interface Config

no poe priority

Use this command to set the priority to the default.

Format	no poe priority
Mode	Interface Config

poe reset

M4250

M4350

Use this command to reset the PoE state of every port (in global mode) or a specific port (in interface mode). When the PoE port status is shown to be in an error state, this command can be used to reset the PoE port. The command can also reset the power-delivering ports. Note that this command takes effect only once after it is executed and cannot be saved across power cycles.

Format	<code>poe reset</code>
Mode	Global Config Interface Config

poe timer schedule

M4250

M4350

Use this command to allow you to attach a timer schedule to a PoE port.

You can define a time schedule using the existing time range commands. This schedule has start and stop times. When this timer schedule is applied to a PoE-enabled port, the capability of the port to deliver power is affected. At the scheduled start time, the PoE port is disabled such that it cannot deliver any power. At the scheduled stop time, the PoE port is reenabled so that it can deliver power.

Note: For information about creating a timer schedule, see [Time Range Commands for Time-Based ACLs](#) on page 1349.

Format	<code>poe timer schedule <i>name</i></code>
Mode	Interface Config

no poe timer schedule name

Use this command to detach the schedule from the port.

Format	<code>no poe timer schedule</code>
Mode	Interface Config

poe usagethreshold (M4250 series switch)

M4250

Use this command to set a threshold (as a percentage) for the total amount of power that can be delivered by the switch. For example, if the switch can deliver up to a maximum of 300 watts, a usage threshold of 90 percent ensures that only 270 watts are used for delivering power to devices. This ensures that more power is not drawn than the switch can provide.

When the usage threshold is set, all the PDs are brought down and then brought back up. If the consumed power is less than the threshold power (in the preceding case, 270 watts), then the devices continue to power up. If the consumed power is 269 watts or less, the next device is powered up. The moment consumed power exceeds the threshold power (270 watts), no other devices can power up.

This command allows you to set the usage threshold based on each individual PoE unit or all PoE units.

Default	90
Format	<code>poe usagethreshold <i>percentage</i></code>
Mode	Global Config

no poe usagethreshold (M4250 series switch)

Use this command to set the usage threshold to a default value.

Format	<code>no poe usagethreshold</code>
Mode	Global Config

poe usagethreshold (M4350 series switch)

M4350

Use this command to set a threshold (as a percentage) for the total amount of power that can be delivered by the switch. For example, if the switch can deliver up to a maximum of 300 watts, a usage threshold of 90 percent ensures that only 270 watts are used for delivering power to devices. This ensures that more power is not drawn than the switch can provide.

When the usage threshold is set, all the PDs are brought down and then brought back up. If the consumed power is less than the threshold power (in the preceding case, 270 watts), then the devices continue to power up. If the consumed power is 269 watts or less, the next device is powered up. The moment consumed power exceeds the threshold power (270 watts), no other devices can power up.

This command allows you to set the usage threshold based on each individual PoE unit or all PoE units.

Default	90
Format	<code>poe usagethreshold {unit all} percentage</code>
Mode	Global Config

`no poe usagethreshold` (M4350 series switch)

Use this command to set the usage threshold to a default value.

Format	<code>no poe usagethreshold {unit all}</code>
Mode	Global Config

`poe traps`

M4250

M4350

Use this command to enable logging of specific PoE-related events, such as a PoE port powering a device, the threshold being exceeded, and so on.

Default	Enabled
Format	<code>poe traps</code>
Mode	Global Config

`no poe traps`

Use this command to disable logging the PoE traps.

Format	<code>no poe traps</code>
Mode	Global Config

`show poe`

M4250

M4350

Use this command to get global information regarding the PoE status.

Format	<code>show poe</code>
Mode	Privileged EXEC User EXEC

Fully Managed Switches M4250 and M4350 Series

Term	Definition
Firmware Version	The firmware version of the PoE controller on the switch.
PSE Main Operational Status	Indicates the status of the PoE controller: • ON. Indicates that the PoE controller is actively delivering power. • OFF. Indicates that the PoE controller is not delivering power. • FAULTY. Indicates that the PoE controller is not functioning.
Total Power Available	The maximum amount of power that can be delivered.
Threshold Power	The switch can power up one port, if consumed power is less than this power. That is, the consumed power can be between the total power and threshold power values. The threshold power value is effected by changing the system usage threshold.
Total Power Consumed	The total amount of power being delivered to all the devices plugged into the switch.
Usage Threshold	The usage threshold level.
Power Management Mode	The management mode used by the PoE controller.
Traps	The configured traps.

Command example:

```
(NETGEAR Switch) #show poe
Firmware Version..... 1.2.0.8
PSE Main Operational Status..... OFF
Total Power Available..... 125.0 Watts
Threshold Power..... 112.5 Watts
Total Power Consumed..... 0.0 Watts
Usage Threshold..... 90
Power Management Mode..... Dynamic
Traps..... Enable
```

show poe port configuration

M4250

M4350

Use this command to see how the PoE ports are configured. You can display information based on each individual port or all the ports collectively.

The port corresponds to a physical port:

- For an M4250 series switch, use the argument *slot/port*.

- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Note: By default, a switch that supports PoE++ shows Dot3bt as the High Power Mode. By default, a switch that supports PoE+ shows Dot3at as the High Power Mode.

Format `show poe port configuration [unit/slot/port | all]`

Mode Privileged EXEC
 User EXEC

Command example:

```
(NETGEAR Switch) #show poe port configuration all
```

Admin Intf	Power Mode	Power Priority	Power Limit Limit (mW)	High Power Type	Power Mode	Detection Type	Timer Schedule
0/1	Enable	Low	N/A	Class Based	Dot3at	4Pt-Dot3af	None
0/2	Enable	Low	N/A	Class Based	Dot3at	4Pt-Dot3af	None
0/3	Enable	Low	N/A	Class Based	Dot3at	4Pt-Dot3af	None
0/4	Enable	Low	N/A	Class Based	Dot3at	4Pt-Dot3af	None
0/5	Enable	Low	N/A	Class Based	Dot3at	4Pt-Dot3af	None
0/6	Enable	Low	N/A	Class Based	Dot3at	4Pt-Dot3af	None
0/7	Enable	Low	N/A	Class Based	Dot3at	4Pt-Dot3af	None
0/8	Enable	Low	N/A	Class Based	Dot3at	4Pt-Dot3af	None

Command example:

```
(NETGEAR Switch) #show poe port configuration 1/0/2
```

Admin Intf	Power Mode	Power Priority	Power Limit Limit (mW)	High Power Type	Power Mode	Detection Type	Timer Schedule
1/0/2	Enable	Low	N/A	Class Based	Dot3at	4Pt-Dot3af	None

show poe port info

M4250

M4350

Use this command to get information about the status of the PoE ports. You can display information based on each individual port or all the ports collectively. The command displays only PSE-capable ports. The port corresponds to a physical port:

- For an M4250 series switch, use the argument *slot/port*.

- For an M4350 series switch, use the argument *unit/slot/port*, as shown in the command format.

Format	show poe port info [<i>unit/slot/port</i> all]
Mode	Privileged EXEC User EXEC
Term	Definition
Intf	Interface on which PoE is configured.
High Power	Indicates if the port supports high power: Yes. The port is capable of supporting 802.3at, 802.3bt, and UPoE. No. The port is capable of supporting 802.3af.
Max Power (mW)	The maximum power allowed in milliwatts.
Class	Class of the powered device according to the 802.3af, 802.3at, and—if supported by the switch—802.3bt definition.
Power (mW)	The actual power delivered in milliwatts.
Output Current (mA)	The current supplied to the powered device (in mA).
Output Voltage (V)	The voltage supplied to the powered device (in volts).
Status	The Status field reports the state of power supplied to the port. The possible values are: - Disabled. The PoE function is disabled on this port. - Searching. The port is detecting the PoE device. - Delivering Power. The port is providing power to the PoE device. - Fault. The PoE device is not IEEE compliant; no power is provided. - Test. The port is in testing state. - Other Fault. The port has experienced problems other than compliance issues. When a port begins to deliver power, there is a trap indicating so. When a port stops delivering power, there is a trap indicating so.
Fault Status	Indicates if the PoE port is in an error state.

Command example:

```
(NETGEAR Switch) #show poe port info all
```

Intf	High Power	Max Power (mW)	Class	Power (mW)	Output Current (mA)	Output Voltage (V)	Status	Fault Status
0/1	Yes	32000	Unknown	0	0	0	Searching	No Error
0/2	Yes	32000	4	4000	74	54	Delivering Power	No Error
0/3	Yes	32000	Unknown	0	0	0	Searching	No Error
0/4	Yes	32000	Unknown	0	0	0	Searching	No Error
0/5	Yes	32000	3	3000	56	53	Delivering Power	No Error
0/6	Yes	32000	4	3800	72	53	Delivering Power	No Error
0/7	Yes	32000	3	1500	28	53	Delivering Power	No Error
0/8	Yes	32000	Unknown	0	0	0	Searching	No Error

Fully Managed Switches M4250 and M4350 Series

Command example:

```
((NETGEAR Switch))#show poe port info 0/2
```

Intf	High Power	Max Power (mW)	Class	Power (mW)	Output Current (mA)	Output Voltage (V)	Status	Fault Status
0/2	Yes	32000	4	4200	78	54	Delivering Power	No Error

Overload Counter	0
Short Counter	0
Power Denied Counter	0
Absent Counter	0
Invalid Signature Counter	0

15

Switch Software Log Messages

This chapter lists common log messages that are provided by the switch, along with information regarding the cause of each message. There is no specific action that can be taken per message. When there is a problem being diagnosed, a set of these messages in the event log, along with an understanding of the system configuration and details of the problem can assist NETGEAR in determining the root cause of such a problem. The most recent log messages are displayed first.

Note: This chapter is not a complete list of all syslog messages.

The chapter includes the following sections:

- [Core](#)
- [Utilities](#)
- [Management](#)
- [Switching](#)
- [QoS](#)
- [Routing/IPv6 Routing](#)
- [Multicast](#)
- [Technologies](#)
- [O/S Support](#)

Core

Table 15. BSP Log Messages

Component	Message	Cause
BSP	Event(0xaaaaaaaa)	Switch has restarted.
BSP	Starting code...	BSP initialization complete, starting the switch.

Table 16. NIM Log Messages

Component	Message	Cause
NIM	NIM: L7_ATTACH out of order for interface unit x port x	Interface creation out of order.
NIM	NIM: Failed to find interface at unit x port x for event(x)	There is no mapping between the USP and Interface number.
NIM	NIM: L7_DETACH out of order for interface unit x port x	Interface creation out of order.
NIM	NIM: L7_DELETE out of order for interface unit x port x	Interface creation out of order.
NIM	NIM: event(x),intf(x),component(x), in wrong phase	An event was issued to NIM during the wrong configuration phase (probably Phase 1, 2, or WMU).
NIM	NIM: Failed to notify users of interface change	Event was not propagated to the system.
NIM	NIM: failed to send message to NIM message Queue.	NIM message queue full or non-existent.
NIM	NIM: Failed to notify the components of L7_CREATE event	Interface not created.
NIM	NIM: Attempted event (x), on USP x.x.x before phase 3	A component issued an interface event during the wrong initialization phase.
NIM	NIM: incorrect phase for operation	An API call was made during the wrong initialization phase.
NIM	NIM: Component(x) failed on event(x) for interface	A component responded with a fail indication for an interface event.
NIM	NIM: Timeout event(x), interface remainingMask = xxxx	A component did not respond before the NIM timeout occurred.

Table 17. SIM Log Message

Component	Message	Cause
SIM	IP address conflict on service port/network port for IP address x.x.x.x. Conflicting host MAC address is xx:xx:xx:xx:xx:xx	This message appears when an address conflict is detected in the LAN for the service port/network port IP.

Table 18. System Log Messages

Component	Message	Cause
SYSTEM	The size of the <code>startup-config.cfg</code> configuration file is 0 (zero) bytes	The configuration file could not be read. This message may occur on a system for which no configuration has ever been saved or for which configuration has been erased.
SYSTEM	could not separate SYSAPI_CONFIG_FILENAME	The configuration file could not be read. This message may occur on a system for which no configuration has ever been saved or for which configuration has been erased.
SYSTEM	Building defaults for file <i>file name</i> version <i>version num</i>	Configuration did not exist or could not be read for the specified feature or file. Default configuration values will be used. The file name and version are indicated.
SYSTEM	File <i>filename</i> : same version (<i>version num</i>) but the sizes (<i>version size</i> – <i>expected version size</i>) differ	The configuration file which was loaded was of a different size than expected for the version number. This message indicates the configuration file needed to be migrated to the version number appropriate for the code image. This message may appear after upgrading the code image to a more current release.
SYSTEM	Migrating config file <i>filename</i> from version <i>version num</i> to <i>version num</i>	The configuration file identified was migrated from a previous version number. Both the old and new version number are specified. This message may appear after upgrading the code image to a more current release.
SYSTEM	Building Defaults	Configuration did not exist or could not be read for the specified feature. Default configuration values will be used.
SYSTEM	sysapiCfgFileGet failed size = <i>expected size of file</i> version = <i>expected version</i>	Configuration did not exist or could not be read for the specified feature. This message is usually followed by a message indicating that default configuration values will be used.

Utilities

Table 19. Trap Mgr Log Message

Component	Message	Cause
Trap Mgr	Link Up/Down: slot/port (M4250 series switch) or unit/slot/port (M4350 series switch)	An interface changed link state.

Table 20. DHCP Filtering Log Messages

Component	Message	Cause
DHCP Filtering	Unable to create r/w lock for DHCP Filtering	Unable to create semaphore used for dhcp filtering configuration structure.
DHCP Filtering	Failed to register with nv Store.	Unable to register save and restore functions for configuration save.
DHCP Filtering	Failed to register with NIM	Unable to register with NIM for interface callback functions.
DHCP Filtering	Error on call to sysapiCfgFileWrite file	Error on trying to save configuration.

Table 21. NVStore Log Messages

Component	Message	Cause
NVStore	Building defaults for file XXX	A component's configuration file does not exist or the file's checksum is incorrect so the component's default configuration file is built.
NVStore	Error on call to osapiFsWrite routine on file XXX	Either the file cannot be opened or the OS's file I/O returned an error trying to write to the file.
NVStore	File XXX corrupted from file system. Checksum mismatch.	The calculated checksum of a component's configuration file in the file system did not match the checksum of the file in memory.
NVStore	Migrating config file XXX from version Y to Z	A configuration file version mismatch was detected so a configuration file migration has started.

Table 22. RADIUS Log Messages

Component	Message	Cause
RADIUS	RADIUS: Invalid data length - xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Failed to send the request	A problem communicating with the RADIUS server.
RADIUS	RADIUS: Failed to send all of the request	A problem communicating with the RADIUS server during transmit.
RADIUS	RADIUS: Could not get the Task Sync semaphore!	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Buffer is too small for response processing	RADIUS Client attempted to build a response larger than resources allow.
RADIUS	RADIUS: Could not allocate accounting requestInfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Could not allocate requestInfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: osapiSocketRecvFrom returned error	Error while attempting to read data from the RADIUS server.
RADIUS	RADIUS: Accounting-Response failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: User (xxx) needs to respond for challenge	An unexpected challenge was received for a configured user.
RADIUS	RADIUS: Could not allocate a buffer for the packet	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Access-Challenge failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Failed to validate Message-Authenticator, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Access-Accept failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Invalid packet length – xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Response is missing Message-Authenticator, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Server address doesn't match configured server	RADIUS Client received a server response from an unconfigured server.

Table 23. TACACS+ Log Messages

Component	Message	Cause
TACACS+	TACACS+: authentication error, no server to contact	TACACS+ request needed, but no servers are configured.
TACACS+	TACACS+: connection failed to server x.x.x.x	TACACS+ request sent to server x.x.x.x but no response was received.
TACACS+	TACACS+: no key configured to encrypt packet for server x.x.x.x	No key configured for the specified server.
TACACS+	TACACS+: received invalid packet type from server.	Received packet type that is not supported.
TACACS+	TACACS+: invalid major version in received packet.	Major version mismatch.
TACACS+	TACACS+: invalid minor version in received packet.	Minor version mismatch.

Table 24. LLDP Log Message

Component	Message	Cause
LLDP	lldpTask(): invalid message type:xx. xxxxxx:xx	Unsupported LLDP packet received.

Table 25. SNTP Log Message

Component	Message	Cause
SNTP	SNTP: system clock synchronized on %s UTC	Indicates that SNTP has successfully synchronized the time of the switch with the server.

Table 26. DHCPv6 Client Log Messages

Component	Message	Cause
DHCP6 Client	ip6Map dhcp add failed.	This message appears when the update of a DHCP leased IP address to IP6Map fails.
DHCP6 Client	osapiNetAddrV6Add failed on interface xxx.	This message appears when the update of a DHCP leased IP address fails.

Table 26. DHCPv6 Client Log Messages

Component	Message	Cause
DHCPv6 Client	Failed to add DNS Server xxx to DNS Client.	This message appears when the update of a DNSv6 Server address given by the DHCPv6 Server to the DNSv6 Client fails.
DHCPv6 Client	Failed to add Domain name xxx to DNS Client.	This message appears when the update of a DNSv6 Domain name info given by the DHCPv6 Server to the DNSv6 Client fails.

Table 27. DHCPv4 Client Log Messages

Component	Message	Cause
DHCPv4 Client	Unsupported subOption (xxx) in Vendor Specific Option in received DHCP pkt	This message appears when a message is received from the DHCP Server that contains an un-supported Vendor Option.
DHCPv4 Client	Failed to acquire an IP address on xxx; DHCP Server did not respond.	This message appears when the DHCP Client fails to lease an IP address from the DHCP Server.
DHCPv4 Client	DNS name server entry add failed.	This message appears when the update of a DNS Domain name server info given by the DHCP Server to the DNS Client fails.
DHCPv4 Client	DNS domain name list entry addition failed.	This message appears when the update of a DNS Domain name list info given by the DHCP Server to the DNS Client fails.
DHCPv4 Client	Interface xxx Link State is Down. Connect the port and try again.	This message appears when the Network protocol is configured with DHCP without any active links in the Management VLAN.

Management

Table 28. SNMP Log Message

Component	Message	Cause
SNMP	EDB Callback: Unit Join: x.	A new member joined the stack.

Table 29. EmWeb Log Messages

Component	Message	Cause
EmWeb	EMWEB (Telnet): Max number of Telnet login sessions exceeded	A user attempted to connect via telnet when the maximum number of telnet sessions were already active.
EmWeb	EMWEB (SSH): Max number of SSH login sessions exceeded	A user attempted to connect via SSH when the maximum number of SSH sessions were already active.
EmWeb	Handle table overflow	All the available EmWeb connection handles are being used and the connection could not be made.
EmWeb	<i>ConnectionType</i> EmWeb socket accept() failed: errno	Socket accept failure for the specified connection type.
EmWeb	ewsNetHTTPReceive failure in NetReceiveLoop() - closing connection.	Socket receive failure.
EmWeb	EmWeb: connection allocation failed	Memory allocation failure for the new connection.
EmWeb	EMWEB TransmitPending: EWOULDBLOCK error sending data	Socket error on send.
EmWeb	ewaNetHTTPEnd: internal error - handle not in Handle table	EmWeb handle index not valid.
EmWeb	ewsNetHTTPReceive:rcvBufCnt exceeds MAX_QUEUED_RECV_BUFS!	The receive buffer limit has been reached. Bad request or DoS attack.
EmWeb	EmWeb accept: XXXX	Accept function for new SSH connection failed. XXXX indicates the error info.

Table 30. CLI_UTIL Log Messages

Component	Message	Cause
CLI_UTIL	Telnet Send Failed errno = 0x%x	Failed to send text string to the telnet client.
CLI_UTIL	osapiFsDir failed	Failed to obtain the directory information from a volume's directory.

Table 31. WEB Log Messages

Component	Message	Cause
WEB	Max clients exceeded	This message is shown when the maximum allowed java client connections to the switch is exceeded.
WEB	Error on send to sockfd XXXX, closing connection	Failed to send data to the java clients through the socket.
WEB	# (XXXX) Form Submission Failed. No Action Taken.	The form submission failed and no action is taken. XXXX indicates the file under consideration.
WEB	ewaFormServe_file_download() - WEB Unknown return code from tftp download result	Unknown error returned while downloading file using TFTP from web interface.
WEB	ewaFormServe_file_upload() - Unknown return code from tftp upload result	Unknown error returned while uploading file using TFTP from web interface.
WEB	Web UI Screen with unspecified access attempted to be brought up	Failed to get application-specific authorization handle provided to EmWeb/Server by the application in ewsAuthRegister(). The specified web page will be served in read-only mode.

Table 32. CLI_WEB_MGR Log Messages

Component	Message	Cause
CLI_WEB_MGR	File size is greater than 2K	The banner file size is greater than 2K bytes.
CLI_WEB_MGR	No. of rows greater than allowed maximum of XXXX	When the number of rows exceeds the maximum allowed rows.

Table 33. SSHD Log Messages

Component	Message	Cause
SSHD	SSHD: Unable to create the global (data) semaphore	Failed to create semaphore for global data protection.
SSHD	SSHD: Msg Queue is full, event = XXXX	Failed to send the message to the SSHD message queue as message queue is full. XXXX indicates the event to be sent.
SSHD	SSHD: Unknown UI event in message, event = XXXX	Failed to dispatch the UI event to the appropriate SSHD function as it's an invalid event. XXXX indicates the event to be dispatched.
SSHD	sshdApiCnfrCommand: Failed calling sshdIssueCmd.	Failed to send the message to the SSHD message queue.

Table 34. SSLT Log Messages

Component	Message	Cause
SSLT	SSLT: Exceeded maximum, ssltConnectionTask	Exceeded maximum allowed SSLT connections.
SSLT	SSLT: Error creating Secure server socket6	Failed to create secure server socket for IPV6.
SSLT	SSLT: Can't connect to unsecure server at XXXX, result = YYYY, errno = ZZZZ	Failed to open connection to unsecure server. XXXX is the unsecure server socket address. YYYY is the result returned from connect function and ZZZZ is the error code.
SSLT	SSLT: Msg Queue is full, event = XXXX	Failed to send the received message to the SSLT message queue as message queue is full. XXXX indicates the event to be sent.
SSLT	SSLT: Unknown UI event in message, event = XXXX	Failed to dispatch the received UI event to the appropriate SSLT function as it's an invalid event. XXXX indicates the event to be dispatched.
SSLT	ssltApiCnfrCommand: Failed calling ssltIssueCmd.	Failed to send the message to the SSLT message queue.
SSLT	SSLT: Error loading certificate from file XXXX	Failed while loading the SSL certificate from specified file. XXXX indicates the file from where the certificate is being read.
SSLT	SSLT: Error loading private key from file	Failed while loading private key for SSL connection.
SSLT	SSLT: Error setting cipher list (no valid ciphers)	Failed while setting cipher list.
SSLT	SSLT: Could not delete the SSL semaphores	Failed to delete SSL semaphores during cleanup of all resources associated with the OpenSSL Locking semaphores.

Table 35. User_Manager Log Messages

Component	Message	Cause
User_Manager	User Login Failed for XXXX	Failed to authenticate user login. XXXX indicates the username to be authenticated.
User_Manager	Access level for user XXXX could not be determined. Setting to READ_ONLY.	Invalid access level specified for the user. The access level is set to READ_ONLY. XXXX indicates the username.
User_Manager	Could not migrate config file XXXX from version YYYY to ZZZZ. Using defaults.	Failed to migrate the config file. XXXX is the config file name. YYYY is the old version number and ZZZZ is the new version number.

Switching

Table 36. Protected Ports Log Messages

Component	Message	Cause
Protected Ports	Protected Port: failed to save configuration	This appears when the protected port configuration cannot be saved.
Protected Ports	protectedPortCnfrgrInitPhase1Process: Unable to create r/w lock for protected Port	This appears when protectedPortCfgRWLock Fails.
Protected Ports	protectedPortCnfrgrInitPhase2Process: Unable to register for VLAN change callback	This appears when nimRegisterIntfChange with VLAN fails.
Protected Ports	Cannot add interface xxx to group yyy	This appears when an interface could not be added to a particular group.
Protected Ports	unable to set protected port group	This appears when a dtl call fails to add interface mask at the driver level.
Protected Ports	Cannot delete interface xxx from group yyy	This appears when a dtl call to delete an interface from a group fails.
Protected Ports	Cannot update group YYY after deleting interface XXX	This message appears when an update group for a interface deletion fails.
Protected Ports	Received an interface change callback while not ready to receive it	This appears when an interface change call back has come before the protected port component is ready.

Table 37. IP Subnet VLANS Log Messages

Component	Message	Cause
IP subnet VLANs	ERROR vlanIpSubnetSubnetValid:Invalid subnet	This occurs when an invalid pair of subnet and netmask has come from the CLI.
IP subnet VLANs	IP Subnet Vlans: failed to save configuration	This message appears when save configuration of subnet vlans failed.
IP subnet VLANs	vlanIpSubnetCnfrgrInitPhase1Process: Unable to create r/w lock for vlanIpSubnet	This appears when a read/write lock creations fails.
IP subnet VLANs	vlanIpSubnetCnfrgrInitPhase2Process: Unable to register for VLAN change callback	This appears when this component unable to register for vlan change notifications.
IP subnet VLANs	vlanIpSubnetCnfrgrFiniPhase1Process: could not delete avl semaphore	This appears when a semaphore deletion of this component fails.
IP subnet VLANs	vlanIpSubnetDtlVlanCreate: Failed	This appears when a dtl call fails to add an entry into the table.

Table 37. IP Subnet VLANS Log Messages

Component	Message	Cause
IP subnet VLANs	vlanIpSubnetSubnetDeleteApply: Failed	This appears when a dtl fails to delete an entry from the table.
IP subnet VLANs	vlanIpSubnetVlanChangeCallback: Failed to add an Entry	This appears when a dtl fails to add an entry for a vlan add notify event.
IP subnet VLANs	vlanIpSubnetVlanChangeCallback: Failed to delete an Entry	This appears when a dtl fails to delete an entry for an vlan delete notify event.

Table 38. Mac-based VLANs Log Messages

Component	Message	Cause
MAC based VLANs	MAC VLANs: Failed to save configuration	This message appears when save configuration of Mac vlans failed.
MAC based VLANs	vlanMacCnfrlInitPhase1Process: Unable to create r/w lock for vlanMac	This appears when a read/write lock creations fails.
MAC based VLANs	Unable to register for VLAN change callback	This appears when this component unable to register for vlan change notifications.
MAC based VLANs	vlanMacCnfrFiniPhase1Process: could not delete avl semaphore	This appears when a semaphore deletion of this component fails.
MAC based VLANs	vlanMacAddApply: Failed to add an entry	This appears when a dtl call fails to add an entry into the table.
MAC based VLANs	vlanMacDeleteApply: Unable to delete an Entry	This appears when a dtl fails to delete an entry from the table.
MAC based VLANs	vlanMacVlanChangeCallback: Failed to add an entry	This appears when a dtl fails to add an entry for a vlan add notify event.
MAC based VLANs	vlanMacVlanChangeCallback: Failed to delete an entry	This appears when a dtl fails to delete an entry for an vlan delete notify event.

Table 39. 802.1X Log Messages

Component	Message	Cause
802.1X	<i>function</i> : Failed calling dot1xIssueCmd	802.1X message queue is full.
802.1X	<i>function</i> : EAP message not received from server	RADIUS server did not send required EAP message.
802.1X	<i>function</i> : Out of System buffers	802.1X cannot process/transmit message due to lack of internal buffers.
802.1X	<i>function</i> : could not set state to <i>authorized/unauthorized</i> , intf xxx	DTL call failed setting authorization state of the port.

Table 39. 802.1X Log Messages

Component	Message	Cause
802.1X	dot1xApplyConfigData: Unable to <i>enable/disable</i> dot1x in driver	DTL call failed enabling/disabling 802.1X.
802.1X	dot1xSendRespToServer: dot1xRadiusAccessRequestSend failed	Failed sending message to RADIUS server.
802.1X	dot1xRadiusAcceptProcess: error calling radiusAccountingStart, ifIndex = xxx	Failed sending accounting start to RADIUS server.
802.1X	<i>function</i> : failed sending terminate cause, intf xxx	Failed sending accounting stop to RADIUS server.

Table 40. IGMP Snooping Log Messages

Component	Message	Cause
IGMP Snooping	<i>function</i> : osapiMessageSend failed	IGMP Snooping message queue is full.
IGMP Snooping	Failed to set global igmp snooping mode to xxx	Failed to set global IGMP Snooping mode due to message queue being full.
IGMP Snooping	Failed to set igmp snooping mode xxx for interface yyy	Failed to set interface IGMP Snooping mode due to message queue being full.
IGMP Snooping	Failed to set igmp mrouter mode xxx for interface yyy	Failed to set interface multicast router mode due to IGMP Snooping message queue being full.
IGMP Snooping	Failed to set igmp snooping mode xxx for vlan yyy	Failed to set VLAN IGM Snooping mode due to message queue being full.
IGMP Snooping	Failed to set igmp mrouter mode%d for interface xxx on Vlan yyy	Failed to set VLAN multicast router mode due to IGMP Snooping message queue being full.
IGMP Snooping	snoopCnfrgInitPhase1Process: Error allocating small buffers	Could not allocate buffers for small IGMP packets.
IGMP Snooping	snoopCnfrgInitPhase1Process: Error allocating large buffers	Could not allocate buffers for large IGMP packets.

Table 41. GARP/GVRP/GMRP Log Messages

Component	Message	Cause
GARP/GVRP/ GMRP	garpSpanState, garpIfStateChange, GarpIssueCmd, garpDot1sChangeCallBack, garpApiCnfrgCommand, garpLeaveAllTimerCallback, garpTimerCallback: QUEUE SEND FAILURE:	The garpQueue is full, logs specifics of the message content like internal interface number, type of message, etc.
GARP/GVRP/ GMRP	GarpSendPDU: QUEUE SEND FAILURE	The garpPduQueue is full, logs specific of the GPDU, internal interface number, vlan id, buffer handle, etc.

Table 41. GARP/GVRP/GMRP Log Messages

Component	Message	Cause
GARP/GVRP/ GMRP	garpMapIntflsConfigurable, gmrpMapIntflsConfigurable: Error accessing GARP/GMRP config data for interface %d in garpMapIntflsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.
GARP/GVRP/ GMRP	garpTraceMsgQueueUsage: garpQueue usage has exceeded fifty/eighty/ninety percent	Traces the build up of message queue. Helpful in determining the load on GARP.
GARP/GVRP/ GMRP	gid_destroy_port: Error Removing port %d registration for vlan-mac %d - %02X:%02X:%02X:%02X:%02X:%02X	Mismatch between the gmd (gmrp database) and MFDB.
GARP/GVRP/ GMRP	gmd_create_entry: GMRP failure adding MFDB entry: vlan %d and address %s	MFDB table is full.

Table 42. 802.3ad Log Messages

Component	Message	Cause
802.3ad	dot3adReceiveMachine: received default event %x	Received a LAG PDU and the RX state machine is ignoring this LAGPDU.
802.3ad	dot3adNimEventCompletionCallback, dot3adNimEventCreateCompletionCallback: DOT3AD: notification failed for event(%d), intf(%d), reason(%d)	The event sent to NIM was not completed successfully.

Table 43. FDB Log Message

Component	Message	Cause
FDB	fdbSetAddressAgingTimeOut: Failure setting fid %d address aging timeout to %d	Unable to set the age time in the hardware.

Table 44. Double VLAN Tag Log Message

Component	Message	Cause
Double Vlan Tag	dvlantagIntflsConfigurable: Error accessing dvlantag config data for interface %d	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.

Table 45. IPv6 Provisioning Log Message

Component	Message	Cause
IPv6 Provisioning	ipv6ProvIntflsConfigurable: Error accessing IPv6 Provisioning config data for interface %d	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.

Table 46. MFDB Log Message

Component	Message	Cause
MFDB	mfdbTreeEntryUpdate: entry does not exist	Trying to update a non existing entry.

Table 47. 802.1Q Log Messages

Component	Message	Cause
802.1Q	dot1qIssueCmd: Unable to send message %d to dot1qMsgQueue for vlan %d - %d msgs in queue	dot1qMsgQueue is full.
802.1Q	dot1qVlanCreateProcess: Attempt to create a vlan with an invalid vlan id %d ; VLAN %d not in range,	This accommodates for reserved vlan ids. i.e. 4094 - x.
802.1Q	dot1qMapIntflsConfigurable: Error accessing DOT1Q config data for interface %d in dot1qMapIntflsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.
802.1Q	dot1qVlanDeleteProcess: Deleting the default VLAN	Typically encountered during clear Vlan and clear config.
802.1Q	dot1qVlanMemberSetModify, dot1qVlanTaggedMemberSetModify: Dynamic entry %d can only be modified after it is converted to static	If this vlan is a learnt via GVRP then we cannot modify its member set via management.
802.1Q	dtl failure when adding ports to vlan id %d - portMask = %s	Failed to add the ports to VLAN entry in hardware.
802.1Q	dtl failure when deleting ports from vlan id %d - portMask = %s	Failed to delete the ports for a VLAN entry from the hardware.
802.1Q	dtl failure when adding ports to tagged list for vlan id %d - portMask = %s	Failed to add the port to the tagged list in hardware.
802.1Q	dtl failure when deleting ports from tagged list for vlan id %d - portMask = %s"	Failed to delete the port to the tagged list from the hardware.
802.1Q	dot1qTask: unsuccessful return code on receive from dot1qMsgQueue: %08x"	Failed to receive the dot1q message from dot1q message queue.
802.1Q	Unable to apply VLAN creation request for VLAN ID %d, Database reached MAX VLAN count!	Failed to create VLAN ID, VLAN Database reached maximum values.

Table 47. 802.1Q Log Messages (continued)

Component	Message	Cause
802.1Q	Attempt to create a vlan (%d) that already exists	Creation of the existing Dynamic VLAN ID from the CLI.
802.1Q	DTL call to create VLAN %d failed with rc %d"	Failed to create VLAN ID in hardware.
802.1Q	Problem unrolling data for VLAN %d	Failed to delete VLAN from the VLAN database after failure of VLAN hardware creation.
802.1Q	Vlan %d does not exist	Failed to delete VLAN entry.
802.1Q	Vlan %d requestor type %d does not exist	Failed to delete dynamic VLAN ID if the given requestor is not valid.
802.1Q	Can not delete the VLAN, Some unknown component has taken the ownership!	Failed to delete, as some unknown component has taken the ownership.
802.1Q	Not valid permission to delete the VLAN %d requestor %d	Failed to delete the VLAN ID as the given requestor and VLAN entry status are not same.
802.1Q	VLAN Delete Call failed in driver for vlan %d	Failed to delete VLAN ID from the hardware.
802.1Q	Problem deleting data for VLAN %d	Failed to delete VLAN ID from the VLAN database.
802.1Q	Dynamic entry %d can only be modified after it is converted to static	Failed to modify the VLAN group filter
802.1Q	Cannot find vlan %d to convert it to static	Failed to convert Dynamic VLAN to static VLAN. VLAN ID not exists.
802.1Q	Only Dynamically created VLANs can be converted	Error while trying to convert the static created VLAN ID to static.
802.1Q	Cannot modify tagging of interface %s to non existence vlan %d"	Error for a given interface sets the tagging property for all the VLANs in the vlan mask.
802.1Q	Error in updating data for VLAN %d in VLAN database	Failed to add VLAN entry into VLAN database.
802.1Q	DTL call to create VLAN %d failed with rc %d	Failed to add VLAN entry in hardware.
802.1Q	Not valid permission to delete the VLAN %d	Failed to delete static VLAN ID. Invalid requestor.
802.1Q	Attempt to set access vlan with an invalid vlan id %d	Invalid VLAN ID.
802.1Q	Attempt to set access vlan with (%d) that does not exist	VLAN ID not exists.
802.1Q	VLAN create currently underway for VLAN ID %d	Creating a VLAN which is already under process of creation.
802.1Q	VLAN ID %d is already exists as static VLAN	Trying to create already existing static VLAN ID.
802.1Q	Cannot put a message on dot1q msg Queue, Returns:%d	Failed to send Dot1q message on Dot1q message Queue.

Table 47. 802.1Q Log Messages (continued)

Component	Message	Cause
802.1Q	Invalid dot1q Interface: %s	Failed to add VLAN to a member of port.
802.1Q	Cannot set membership for user interface %s on management vlan %d	Failed to add VLAN to a member of port.
802.1Q	Incorrect tagmode for vlan tagging. tagmode: %d Interface: %s	Incorrect tagmode for VLAN tagging.
802.1Q	Cannot set tagging for interface %d on non existent VLAN %d"	The VLAN ID does not exist.
802.1Q	Cannot set tagging for interface %d which is not a member of VLAN %d	Failure in Setting the tagging configuration for a interface on a range of VLAN.
802.1Q	VLAN create currently underway for VLAN ID %d"	Trying to create the VLAN ID which is already under process of creation.
802.1Q	VLAN ID %d already exists	Trying to create the VLAN ID which is already exists.
802.1Q	Failed to delete, Default VLAN %d cannot be deleted	Trying to delete Default VLAN ID.
802.1Q	Failed to delete, VLAN ID %d is not a static VLAN	Trying to delete Dynamic VLAN ID from CLI.
802.1Q	Requestor %d attempted to release internal VLAN %d: owned by %d	-

Table 48. 802.1S Log Messages

Component	Message	Cause
802.1S	dot1sIssueCmd: Dot1s Msg Queue is full!!!!Event: %u, on interface: %u, for instance: %u	The message Queue is full.
802.1S	dot1sStateMachineRxBpdu(): Rcvd BPDU Discarded	The current conditions, like port is not enabled or we are currently not finished processing another BPDU on the same interface, does not allow us to process this BPDU.
802.1S	dot1sBpduTransmit(): could not get a buffer	Out of system buffers.

Table 49. Port Mac Locking Log Message

Component	Message	Cause
Port Mac Locking	pmlMapIntflsConfigurable: Error accessing PML config data for interface %d in pmlMapIntflsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.

Table 50. Protocol-based VLANs Log Messages

Component	Message	Cause
Protocol Based VLANs	pbVlanCnfrgrInitPhase2Process: Unable to register NIM callback	Appears when nimRegisterIntfChange fails to register pbVlan for link state changes.
Protocol Based VLANs	pbVlanCnfrgrInitPhase2Process: Unable to register pbVlan callback with VLANs	Appears when VLANRegisterForChange fails to register pbVlan for VLAN changes.
Protocol Based VLANs	pbVlanCnfrgrInitPhase2Process: Unable to register pbVlan callback with nvStore	Appears when nvStoreRegister fails to register save and restore functions for configuration save.

QoS

Table 51. ACL Log Messages

Component	Message	Cause
ACL	Total number of ACL rules (x) exceeds max (y) on intf i.	The combination of all ACLs applied to an interface has resulted in requiring more rules than the platform supports.
ACL	ACL <i>name</i> , rule x: This rule is not being logged	The ACL configuration has resulted in a requirement for more logging rules than the platform supports. The specified rule is functioning normally except for the logging action.
ACL	aclLogTask: error logging ACL rule trap for correlator <i>number</i>	The system was unable to send an SNMP trap for this ACL rule which contains a logging attribute.
ACL	IP ACL <i>number</i> : Forced truncation of one or more rules during config migration	While processing the saved configuration, the system encountered an ACL with more rules than is supported by the current version. This may happen when code is updated to a version supporting fewer rules per ACL than the previous version.

Table 52. CoS Log Message

Component	Message	Cause
COS	cosCnfrgrInitPhase3Process: Unable to apply saved config -- using factory defaults	The COS component was unable to apply the saved configuration and has initialized to the factory default settings.

Table 53. DiffServ Log Messages

Component	Message	Cause
DiffServ	diffserv.c 165: diffServRestore Failed to reset DiffServ. Recommend resetting device	While attempting to clear the running configuration an error was encountered in removing the current settings. This may lead to an inconsistent state in the system and resetting is advised.
DiffServ	Policy invalid for service intf: policy <i>name</i> , interface <i>x</i> , direction <i>y</i>	The DiffServ policy definition is not compatible with the capabilities of the interface specified. Check the platform release notes for information on configuration limitations.

Routing/IPv6 Routing

Table 54. DHCP Relay Log Messages

Component	Message	Cause
DHCP relay	REQUEST hops field more than config value	The DHCP relay agent has processed a DHCP request whose HOPS field is larger than the maximum value allowed. The relay agent will not forward a message with a hop count greater than 4.
DHCP relay	Request's seconds field less than the config value	The DHCP relay agent has processed a DHCP request whose SECS field is larger than the configured minimum wait time allowed.
DHCP relay	processDhcpPacket: invalid DHCP packet type: %u\n	The DHCP relay agent has processed an invalid DHCP packet. Such packets are discarded by the relay agent.

Table 55. Routing Table Manager Log Messages

Component	Message	Cause
RTO	RTO is no longer full. Routing table contains xxx best routes, xxx total routes, xxx reserved local routes.	When the number of best routes drops below full capacity, RTO logs this notice. The number of bad adds may give an indication of the number of route adds that failed while RTO was full, but a full routing table is only one reason why this count is incremented.
RTO	RTO is full. Routing table contains xxx best routes, xxx total routes, xxx reserved local routes. The routing table manager stores a limited number of best routes. The count of total routes includes alternate routes, which are not installed in hardware.	The routing table manager, also called "RTO," stores a limited number of best routes, based on hardware capacity. When the routing table becomes full, RTO logs this alert. The count of total routes includes alternate routes, which are not installed in hardware.

Table 56. ARP Log Message

Component	Message	Cause
ARP	IP address conflict on interface xxx for IP address yyy. Conflicting host MAC address is zzz.	When an address conflict is detected for any IP address on the switch upon reception of ARP packet from another host or router.

Table 57. RIP Log Message

Component	Message	Cause
RIP	RIP: discard response from xxx via unexpected interface	When RIP response is received with a source address not matching the incoming interface's subnet.

Multicast

Table 58. IGMP/MLD Log Messages

Component	Message	Cause
IGMP/MLD	MGMD Protocol Heap Memory Init Failed; Family – xxx.	MGMD Heap memory initialization Failed for the specified address family. This message appears when trying to enable MGMD Protocol.
IGMP/MLD	MGMD Protocol Heap Memory De-Init Failed; Family – xxx.	MGMD Heap memory de-initialization Failed for the specified address family. This message appears when trying to disable MGMD (IGMP/MLD) Protocol. As a result of this, the subsequent attempts to enable/disable MGMD will also fail.
IGMP/MLD	MGMD Protocol Initialization Failed; Family – xxx.	MGMD protocol initialization sequence Failed. This could be due to the non-availability of some resources. This message appears when trying to enable MGMD Protocol.
IGMP/MLD	MGMD All Routers Address - xxx Set to the DTL Mcast List Failed; Mode – xxx, intf – xxx.	This message appears when trying to enable/disable MGMD Protocol.
IGMP/MLD	MGMD All Routers Address - xxx Add to the DTL Mcast List Failed.	MGMD All Routers Address addition to the local multicast list Failed. As a result of this, MGMD Multicast packets with this address will not be received at the application.
IGMP/MLD	MGMD All Routers Address – xxx Delete from the DTL Mcast List Failed.	MGMD All Routers Address deletion from the local multicast list Failed. As a result of this, MGMD Multicast packets are still received at the application though MGMD is disabled.
IGMP/MLD	MLDv2 GroupAddr-[FF02::16] Enable with Interpeak Stack Failed; rtrIfNum - xxx, intf – xxx.	Registration of this Group address with the Interpeak stack failed. As a result of this, MLDv2 packets will not be received at the application.
IGMP/MLD	MGMD Group Entry Creation Failed; grpAddr - xxx, rtrIfNum – xxx.	The specified Group Address registration on the specified router interface failed.
IGMP/MLD	MGMD Socket Creation/Initialization Failed for addrFamily – xxx.	MGMD Socket Creation/options Set Failed. As a result of this, the MGMD Control packets cannot be sent out on an interface.

Table 59. IGMP-Proxy Log Messages

Component	Message	Cause
IGMP-Proxy/MLD-Proxy	MGMD-Proxy Protocol Initialization Failed; Family – xxx.	MGMD-Proxy protocol initialization sequence Failed. This could be due to the non-availability of some resources. This message appears when trying to enable MGMD-Proxy Protocol.
IGMP-Proxy/MLD-Proxy	MGMD-Proxy Protocol Heap Memory De-Init Failed; Family – xxx.	MGMD-Proxy Heap memory de-initialization is Failed for the specified address family. This message appears when trying to disable MGMD-Proxy Protocol. As a result of this, the subsequent attempts to enable/disable MGMD-Proxy will also fail.
IGMP-Proxy/MLD-Proxy	MGMD Proxy Route Entry Creation Failed; grpAddr - xxx, srcAddr – xxx, rtrIfNum – xxx.	Registration of the Multicast Forwarding entry for the specified Source and Group Address Failed when MGMD-Proxy is used.

Table 60. PIM-SM Log Messages

Component	Message	Cause
PIMSM	Non-Zero SPT/Data Threshold Rate – xxx is currently Not Supported on this platform.	This message appears when the user tries to configure the PIMSM SPT threshold value.
PIMSM	PIMSM Protocol Heap Memory Init Failed; Family – xxx.	PIMSM Heap memory initialization Failed for the specified address family. This message appears when trying to enable PIMSM Protocol.
PIMSM	PIMSM Protocol Heap Memory De-Init Failed; Family –xxx.	PIMSM Heap memory de-initialization Failed for the specified address family. This message appears when trying to disable PIMSM Protocol. As a result of this, the subsequent attempts to enable/disable PIMSM will also fail.
PIMSM	PIMSM Protocol Initialization Failed; Family –xxx.	PIMSM protocol initialization sequence Failed. This could be due to the non-availability of some resources. This message appears when trying to enable PIMSM Protocol.
PIMSM	PIMSM Protocol De-Initialization Failed; Family – xxx.	PIMSM protocol de-initialization sequence Failed. This message appears when trying to disable PIMSM Protocol.
PIMSM	PIMSM SSM Range Table is Full.	PIMSM SSM Range Table is Full. This message appears when the protocol cannot accommodate new SSM registrations.
PIMSM	PIM All Routers Address – xxx Delete from the DTL Mcast List Failed for intf – xxx.	PIM All Routers Address deletion from the local multicast list Failed. As a result of this, PIM Multicast packets are still received at the application though PIM is disabled.

Table 60. PIM-SM Log Messages (continued)

Component	Message	Cause
PIMSM	PIM All Routers Address - xxx Add to the DTL Mcast List Failed for intf – xxx.	PIM All Routers Address addition to the local multicast list Failed. As a result of this, PIM Multicast packets with this address will not be received at the application.
PIMSM	Mcast Forwarding Mode Disable Failed for intf – xxx.	Multicast Forwarding Mode Disable Failed. As a result of this, Multicast packets are still received at the application though no protocol is enabled.
PIMSM	Mcast Forwarding Mode Enable Failed for intf – xxx.	Multicast Forwarding Mode Enable Failed. As a result of this, Multicast packets will not be received at the application though a protocol is enabled.
PIMSM	PIMSMv6 Socket Memb'ship Enable Failed for rtrIfNum - xxx.	PIMSMv6 Socket Creation/options Set with Kernel IP Stack Failed. As a result of this, the PIM Control packets cannot be received on the interface.
PIMSM	PIMSMv6 Socket Memb'ship Disable Failed for rtrIfNum – xxx.	PIMSMv6 Socket Creation/options Disable with Kernel IP Stack Failed. As a result of this, the PIM Control packets are still received on the interface at the application though no protocol is enabled.
PIMSM	PIMSM (S,G,RPt) Table Max Limit – xxx Reached; Cannot accommodate any further routes.	PIMSM Multicast Route table (S,G,RPt) has reached maximum capacity and cannot accommodate new registrations anymore.
PIMSM	PIMSM (S,G) Table Max Limit - xxx Reached; Cannot accommodate any further routes.	PIMSM Multicast Route table (S,G) has reached maximum capacity and cannot accommodate new registrations anymore.
PIMSM	PIMSM (*,G) Table Max Limit - xxx Reached; Cannot accommodate any further routes.	PIMSM Multicast Route table (*,G) has reached maximum capacity and cannot accommodate new registrations anymore.

Table 61. PIM-DM Log Messages

Component	Message	Cause
PIMDM	PIMDM Protocol Heap Memory Init Failed; Family – xxx.	PIMDM Heap memory initialization Failed for the specified address family. This message appears when trying to enable PIMDM Protocol.
PIMDM	PIMDM Protocol Heap Memory De-Init Failed; Family –xxx.	PIMDM Heap memory de-initialization Failed for the specified address family. This message appears when trying to disable PIMDM Protocol. As a result of this, the subsequent attempts to enable/disable PIMDM will also fail.

Table 61. PIM-DM Log Messages (continued)

Component	Message	Cause
PIMDM	PIMDM Protocol Initialization Failed; Family –xxx.	PIMDM protocol initialization sequence Failed. This could be due to the non-availability of some resources. This message appears when trying to enable PIMDM Protocol.
PIMDM	PIMDM Protocol De-Initialization Failed; Family –xxx.	PIMDM protocol de-initialization sequence Failed. This message appears when trying to disable PIMDM Protocol.
PIMDM	PIM All Routers Address – xxx Delete from the DTL Mcast List Failed for intf – xxx.	PIM All Routers Address deletion from the local multicast list Failed. As a result of this, PIM Multicast packets are still received at the application though PIM is disabled.
PIMDM	PIM All Routers Address - xxx Add to the DTL Mcast List Failed for intf – xxx.	PIM All Routers Address addition to the local multicast list Failed. As a result of this, PIM Multicast packets with this address will not be received at the application.
PIMDM	Mcast Forwarding Mode Disable Failed for intf – xxx.	Multicast Forwarding Mode Disable Failed. As a result of this, Multicast packets are still received at the application though no protocol is enabled.
PIMDM	Mcast Forwarding Mode Enable Failed for intf – xxx.	Multicast Forwarding Mode Enable Failed. As a result of this, Multicast packets will not be received at the application though a protocol is enabled.
PIMDM	PIMDMv6 Socket Memb'ship Enable Failed for rtrIfNum - xxx.	PIMDMv6 Socket Creation/options Set with Kernel IP Stack Failed. As a result of this, the PIM Control packets cannot be received on the interface.
PIMDM	PIMDMv6 Socket Memb'ship Disable Failed for rtrIfNum – xxx.	PIMDMv6 Socket Creation/options Disable with Kernel IP Stack Failed. As a result of this, the PIM Control packets are still received on the interface at the application though no protocol is enabled.
PIMDM	PIMDM FSM Action Invoke Failed; rtrIfNum - xxx Out of Bounds for Event – xxx.	The PIMDM FSM Action invocation Failed due to invalid Routing interface number. In such cases, the FSM Action routine can never be invoked which may result in abnormal behavior. The failed FSM-name can be identified from the specified Event name.
PIMDM	PIMDM Socket Initialization Failed for addrFamily - xxx.	PIMDM Socket Creation/options Set Failed. As a result of this, the PIM Control packets cannot be sent out on an interface.
PIMDM	PIMDMv6 Socket Memb'ship Enable Failed for rtrIfNum - xxx.	Socket options Set to enable the reception of PIMv6 packets Failed. As a result of this, the PIMv6 packets will not be received by the application.

Table 61. PIM-DM Log Messages (continued)

Component	Message	Cause
PIMDM	PIMDMv6 Socket Memb'ship Disable Failed for rtrIfNum – xxx.	PIMDMv6 Socket Creation/options Disable with Kernel IP Stack Failed. As a result of this, the PIMv6 Control packets are still received on the interface at the application though no protocol is enabled.
PIMDM	PIMDM MRT Table Max Limit - xxx Reached; Cannot accommodate any further routes.	PIMDM Multicast Route table (S,G) has reached maximum capacity and cannot accommodate new registrations anymore.

Technologies

Table 62. Error Messages

Component	Message	Cause
OS	Invalid USP unit = x, port = x	A port was not able to be translated correctly during the receive.
OS	In hapiBroadSystemMacAddress call to 'bcm_l2_addr_add' - FAILED : x	Failed to add an L2 address to the MAC table. This should only happen when a hash collision occurs or the table is full.
OS	Failed installing mirror action - rest of the policy applied successfully	A previously configured probe port is not being used in the policy. The release notes state that only a single probe port can be configured.
OS	Policy x does not contain rule x	The rule was not added to the policy due to a discrepancy in the rule count for this specific policy. Additionally, the message can be displayed when an old rule is being modified, but the old rule is not in the policy.
OS	ERROR: policy x, tmpPolicy x, size x, data x x x x x x x x	An issue installing the policy due to a possible duplicate hash.
OS	ACL x not found in internal table	Attempting to delete a non-existent ACL.
OS	ACL internal table overflow	Attempting to add an ACL to a full table.
OS	In hapiBroadQosCosQueueConfig, Failed to configure minimum bandwidth. Available bandwidth x	Attempting to configure the bandwidth beyond its capabilities.
OS	USL: failed to put sync response on queue	A response to a sync request was not enqueued. This could indicate that a previous sync request was received after it was timed out.
OS	USL: failed to sync ipmc table on unit = x	Either the transport failed or the message was dropped.

Table 62. Error Messages (continued)

Component	Message	Cause
OS	usl_task_ipmc_msg_send(): failed to send with x	Either the transport failed or the message was dropped.
OS	USL: No available entries in the STG table	The Spanning Tree Group table is full in USL.
OS	USL: failed to sync stg table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
OS	USL: A Trunk doesn't exist in USL	Attempting to modify a Trunk that doesn't exist.
OS	USL: A Trunk being created by bcmx already existed in USL	Possible synchronization issue between the application, hardware, and sync layer.
OS	USL: A Trunk being destroyed doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
OS	USL: A Trunk being set doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
OS	USL: failed to sync trunk table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
OS	USL: Mcast entry not found on a join	Possible synchronization issue between the application, hardware, and sync layer.
OS	USL: Mcast entry not found on a leave	Possible synchronization issue between the application, hardware, and sync layer.
OS	USL: failed to sync dVLAN data on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
OS	USL: failed to sync policy table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
OS	USL: failed to sync VLAN table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
OS	Invalid LAG id x	Possible synchronization issue between the BCM driver and HAPI.
OS	Invalid uport calculated from the BCM uport bcmx_l2_addr->lport = x	Uport not valid from BCM driver.
OS	Invalid USP calculated from the BCM uport\nbcmx_l2_addr->lport = x	USP not able to be calculated from the learn event for BCM driver.
OS	Unable to insert route R/P	Route R with prefix P could not be inserted in the hardware route table. A retry will be issued.

Table 62. Error Messages (continued)

Component	Message	Cause
OS	Unable to Insert host H	Host H could not be inserted in hardware host table. A retry will be issued.
OS	USL: failed to sync L3 Intf table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
OS	USL: failed to sync L3 Host table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
OS	USL: failed to sync L3 Route table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
OS	USL: failed to sync initiator table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
OS	USL: failed to sync terminator table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
OS	USL: failed to sync ip-multicast table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.

O/S Support

Table 63. BSP Log Message

Component	Message	Cause
BSP	rc = 10	Second message logged at bootup, right after <i>Starting code.... Always</i> logged.

Table 64. OSAPI Log Messages

Component	Message	Cause
OSAPI	osapiNetLinkNeighDump: could not open socket! - or – ipstkNdpFlush: could not open socket! – or – osapiNetlinkDumpOpen: unable to bind socket! errno = XX	Couldn't open a netlink socket. Make sure "ARP Daemon support" (CONFIG_ARPD) is enabled in the kernel, if the reference kernel binary is not being used.
OSAPI	ipstkNdpFlush: sending delete failed	Failed when telling the kernel to delete a neighbor table entry (the message is incorrect).
OSAPI	unable to open /proc/net/ipv6/conf/default/hop_limit	IPv6 MIB objects read, but /proc file system is not mounted, or running kernel does not have IPV6 support.
OSAPI	osapimRouteEntryAdd, errno XX adding 0xYY to ZZ – or – osapimRouteEntryDelete, errno XX deleting 0xYY from ZZ	Error adding or deleting an IPv4 route (listed in hex as YY), on the interface with name ZZ Error code can be looked up in errno.h.
OSAPI	I3intfAddRoute: Failed to Add Route – or – I3intfDeleteRoute: Failed to Delete Route	Error adding or deleting a default gateway in the kernel's routing table (the function is really osapiRawMRouteAdd()/Delete()).
OSAPI	osapiNetIfConfig: ioctl on XX failed: addr: 0xYY, err: ZZ – or – osapiNetIPSet: ioctl on XX failed: addr: 0x%YY	Failed trying to set the IP address (in hex as YY) of the interface with name XX, and the interface does not exist. Sometimes this is a harmless race condition (e.g. we try to set address 0 when DHCPing on the network port (dtl0) at bootup, before it's created using TAP).
OSAPI	ping: sendto error	Trouble sending an ICMP echo request packet for the UI ping command. Maybe there was no route to that network.
OSAPI	Failed to Create Interface	Out of memory at system initialization time.
OSAPI	TAP Unable to open XX	The /dev/tap file is missing, or, if not using the reference kernel binary, the kernel is missing "Universal TUN/TAP device driver support" (CONFIG_TUN).
OSAPI	Tap monitor task is spinning on select failures – then – Tap monitor select failed: XX	Trouble reading the /dev/tap device, check the error message XX for details.
OSAPI	Log_Init: log file error - creating new log file	This pertains to the "event log" persistent file in flash. Either it did not exist, or had a bad checksum.
OSAPI	Log_Init: Flash (event) log full; erasing	Event log file has been cleared; happens at boot time.

Table 64. OSAPI Log Messages (continued)

Component	Message	Cause
OSAPI	Log_Init: Corrupt event log; erasing	Event log file had a non-blank entry after a blank entry; therefore, something was messed up.
OSAPI	Failed to Set Interface IP Address – or – IP Netmask – or – Broadcast Address – or – Flags – or – Hardware Address – or – Failed to Retrieve Interface Flags	Trouble adding MAC address(es) to a network interface.

Command List

.....	551
(NETGEAR Switch)# vlan association oui 00:01:02 9	552
[sequence-number] {deny permit} (IP ACL)	1329
[sequence-number] {deny permit} (MAC ACL)	1315
{deny permit} (IPv6 ACL)	1341
1583compatibility	1014
aaa accounting	154
aaa accounting update	156
aaa authentication dot1x default	616
aaa authentication enable	123
aaa authentication login	122
aaa authorization	125
aaa ias-user username	153
aaa server radius dynamic-author	183
aaa session-id	153
absolute	1350
accept-mode (VRRPv3 Config mode)	987
access-list	1322
accounting	159
acl-trapflags	1335
addport	670
address (VRRPv3 Config mode)	988
address prefix (IPv6 DHCP Pool Config)	1249
address range (DHCP Pool Class Config)	364
application install	228
application start	229
application stop	230
area default-cost (Router OSPF Config)	1015
area default-cost (Router OSPFv3 Config)	1198
area nssa (Router OSPF Config)	1015
area nssa (Router OSPFv3 Config)	1199
area nssa default-info-originate (Router OSPF Config)	1015
area nssa default-info-originate (Router OSPFv3 Config)	1199
area nssa no-redistribute (Router OSPF Config)	1016
area nssa no-redistribute (Router OSPFv3 Config)	1199
area nssa no-summary (Router OSPF Config)	1016
area nssa no-summary (Router OSPFv3 Config)	1200
area nssa translator-role (Router OSPF Config)	1017
area nssa translator-role (Router OSPFv3 Config)	1200
area nssa translator-stab-intv (Router OSPF Config)	1017

area nssa translator-stab-intv (Router OSPFv3 Config)	1201
area range (Router OSPF Config)	1018
area range (Router OSPFv3 Config)	1201
area stub (Router OSPF Config)	1019
area stub (Router OSPFv3 Config)	1202
area stub no-summary (Router OSPF Config)	1020
area stub no-summary (Router OSPFv3 Config)	1202
area virtual-link (Router OSPF Config)	1020
area virtual-link (Router OSPFv3 Config)	1203
area virtual-link authentication	1020
area virtual-link dead-interval (Router OSPF Config)	1021
area virtual-link dead-interval (Router OSPFv3 Config)	1203
area virtual-link hello-interval (Router OSPF Config)	1022
area virtual-link hello-interval (Router OSPFv3 Config)	1204
area virtual-link retransmit-interval (Router OSPF Config)	1022
area virtual-link retransmit-interval (Router OSPFv3 Config)	1204
area virtual-link transmit-delay (Router OSPF Config)	1023
area virtual-link transmit-delay (Router OSPFv3 Config)	1205
arp	906
arp access-list	733
arp cachesize	907
arp dynamicrenew	908
arp purge	911
arp resptime	909
arp retries	909
arp timeout	910
arp-guard attack-threshold	740
arp-guard enable	739
arp-guard rate-limit	739
assign-queue	1299
authentication allow-unauth dhcp	634
authentication command bounce-port ignore	185
authentication command disable-port ignore	185
authentication control-direction	632
authentication critical recovery max-reauth	619
authentication dynamic-vlan enable	621
authentication enable	627
authentication enable	631
authentication event fail action authorize vlan	629
authentication event fail retry	629
authentication event no-response action authorize vlan	622
authentication event server alive action	635
authentication event server dead action	634
authentication host-mode	618
authentication host-mode all	618

authentication max-users	623
authentication monitor	636
authentication open	619
authentication order	632
authentication periodic	626
authentication port-control	617
authentication port-control	624
authentication port-control all	617
authentication priority	633
authentication restart	633
authentication timeout (Captive Portal Config)	1103
authentication timer reauthenticate	626
authentication timer restart	627
authentication violation	635
authorization commands	129
authorization exec	130
authorization exec default	131
authorization network radius	184
auth-type	184
auto-cost (Router OSPF Config)	1023
auto-cost (Router OSPFv3 Config)	1205
auto-default-router (DHCP Pool Config)	357
auto-dos	840
auto-negotiate	482
auto-negotiate all	482
autostate	914
autostate	966
auto-summary (Router RIP Config)	1073
auto-voip	1352
auto-voip oui	1353
auto-voip oui-based priority	1353
auto-voip protocol-based	1354
auto-voip vlan	1355
background-color	1117
bandwidth	1036
block	1116
bonjour run	871
boot auto-copy-sw (for stack firmware synchronization)	50
boot auto-copy-sw allow-downgrade (for stack firmware synchronization)	50
boot auto-copy-sw trap (for stack firmware synchronization)	50
boot autoinstall	250
boot host autoreboot	251
boot host autosave	251
boot host dhcp	250

boot host retrycount	250
boot system	256
bootfile (DHCP Pool Class Config)	365
bootfile (DHCP Pool Config)	354
bootpdhcprelay cidoptmode	1000
bootpdhcprelay maxhopcount	1000
bootpdhcprelay minwaittime	1000
bootpdhcprelay server-override	1001
bootpdhcprelay source-interface	1002
bridge aging-time	841
cablestatus	426
capability opaque	1024
captive-portal	1101
captive-portal client deauthenticate	1125
capture {file remote line usb}	380
capture file size	381
capture line wrap	381
capture remote port	381
capture start	379
capture stop	379
capture usb	382
class	1298
class (DHCP Pool Config)	363
class-map	1287
class-map rename	1288
classofservice dot1p-mapping	1273
classofservice ip-dscp-mapping	1273
classofservice trust	1275
clear (Captive Portal Instance Config)	1116
clear aaa ias-users	158
clear accounting statistics	161
clear arp-cache	911
clear arp-guard attack history	745
clear arp-guard statistics	745
clear arp-switch	911
clear authentication authentication-history	643
clear authentication sessions	620
clear authentication statistics	643
clear captive-portal users	1138
clear checkpoint statistics (for stack configuration)	56
clear config	323
clear counters	324
clear counters keepalive	537
clear dhcp l2relay statistics interface	715
clear dot1as statistics	883

clear dot1x statistics	620
clear eventlog	307
clear green-mode statistics	453
clear host	376
clear igmpsnooping	325
clear ip access-list counters	325
clear ip address-conflict-detect	378
clear ip arp inspection statistics	737
clear ip device tracking	862
clear ip dhcp binding	366
clear ip dhcp conflict	367
clear ip dhcp server statistics	366
clear ip dhcp snooping binding	727
clear ip dhcp snooping statistics	727
clear ip helper statistics	1012
clear ip mroute	1375
clear ip ospf	1024
clear ip ospf configuration	1024
clear ip ospf counters	1025
clear ip ospf neighbor	1025
clear ip ospf neighbor interface	1025
clear ip ospf redistribution	1025
clear ip ospf stub-router	1047
clear ip route (M4250 series switch)	942
clear ip route (M4350 series switch)	942
clear ip sla statistics	1096
clear ip vrrp interface stats	984
clear ipv6 access-list counters	326
clear ipv6 dhcp	1257
clear ipv6 dhcp binding	1258
clear ipv6 dhcp snooping binding	1268
clear ipv6 dhcp snooping statistics	1269
clear ipv6 mld counters	1449
clear ipv6 mld traffic	1449
clear ipv6 mroute	1422
clear ipv6 neighbors	1170
clear ipv6 ospf	1206
clear ipv6 ospf configuration	1206
clear ipv6 ospf counters	1206
clear ipv6 ospf neighbor	1206
clear ipv6 ospf neighbor interface	1207
clear ipv6 ospf redistribution	1207
clear ipv6 ospf stub-router	1227
clear ipv6 pim statistics	1431

clear ipv6 prefix-list	1192
clear ipv6 route counters	1179
clear ipv6 snooping counters	1180
clear ipv6 statistics	1188
clear isdp counters	846
clear isdp table	846
clear lldp remote-data	812
clear lldp statistics	812
clear logging buffered	307
clear logging email statistics	312
clear mac access-list counters	326
clear mac-addr-table	324
clear mbuf stats	424
clear mldsnooping	792
clear mmrp statistics	890
clear msrp statistics	904
clear mvrp	895
clear network ipv6 dhcp statistics	1258
clear openflow ca-cert	235
clear port-channel all counters	692
clear port-channel counters	692
clear radius dynamic-author statistics	186
clear radius statistics	620
clear serviceport ipv6 dhcp statistics	1258
clear traplog	326
clear vlan	326
clear vrrp statistics	999
client	186
client-identifier (DHCP Pool Config)	350
client-name (DHCP Pool Config)	350
clock set	345
clock summer-time date	345
clock summer-time recurring	346
clock timezone	347
cloud-managed	244
configuration (for captive portal)	1107
configure (or config)	76
conform-color	1300
copy	315
copy (pre-login banner)	226
copy nvram:core-dum unit	51
copy nvram:cpu-pkt-capture.pcap unit	51
copy nvram:tech-support unit	52
copy unit	51
cos-queue min-bandwidth	1276

cos-queue random-detect	1277
cos-queue strict	1277
crypto certificate generate	94
crypto certificate import	99
crypto certificate request	97
crypto dhparam size	100
crypto key decrypt write	101
crypto key generate dsa	96
crypto key generate ecdsa	97
crypto key generate rsa	96
crypto key pubkey-chain ssh	101
dampening	1070
dante	1274
dante <i>vlan</i>	1275
debug aaa accounting	382
debug aaa authorization	383
debug aaa coa	186
debug aaa coa	384
debug aaa pod	187
debug aaa pod	384
debug arp	385
debug authentication	385
debug auto-vlan	386
debug auto-voip	386
debug bonjour	872
debug clear	387
debug console	387
debug crashlog (M4250 series switch)	387
debug crashlog (M4350 series switch)	389
debug debug-config	390
debug dhcp packet	390
debug dhcp server packet	391
debug dot1x packet	391
debug drop-counters show	392
debug drop-counters start	392
debug drop-counters stop	392
debug dynamic ports	492
debug exception	421
debug igmpsnooping packet	393
debug igmpsnooping packet receive	394
debug igmpsnooping packet transmit	393
debug ip acl	395
debug ip dvmrp packet	396
debug ip igmp packet	396

debug ip mcache packet	397
debug ip pimdm packet	397
debug ip pimsm packet	398
debug ip vrrp	413
debug ipdt logging	413
debug ipv6 dhcp	399
debug ipv6 mcache packet	399
debug ipv6 mld packet	400
debug ipv6 ospfv3 packet	414
debug ipv6 pimdm packet	400
debug ipv6 pimsm packet	401
debug ipv6 ping packet	414
debug isdp packet	852
debug lacp packet	402
debug lldp packet	402
debug mldsnooping packet	403
debug mvr packet	754
debug mvr trace	754
debug ospf packet	404
debug ping packet	403
debug rip packet	406
debug sflow packet	408
debug spanning-tree bpdu	408
debug spanning-tree bpdu receive	409
debug spanning-tree bpdu transmit	410
debug tacacs	411
debug transfer	411
debug udd events	412
debug udd packet	412
default-information originate (Router OSPF Config)	1026
default-information originate (Router OSPFv3 Config)	1207
default-information originate (Router RIP Config)	1074
default-metric (Router OSPF Config)	1026
default-metric (Router OSPFv3 Config)	1208
default-metric (Router RIP Config)	1074
default-router (DHCP Pool Config)	351
delay (Track Config)	1088
delete	256
deleteport (Global Config)	671
deleteport (Interface Config)	670
deny permit ip-source (Management access-list configuration)	108
deny ip host mac host	734
deny lease (DHCP Pool Class Config)	365
description (Interface Config)	483
destination (ERSPAN Source Session Config)	700

dhcp client vendor-id-option	716
dhcp client vendor-id-option-string	716
dhcp l2relay	709
dhcp l2relay circuit-id	711
dhcp l2relay circuit-id vlan	709
dhcp l2relay remote-id	710
dhcp l2relay trust	711
dhcp l2relay vlan	710
diffserv	1286
dir	291
dir usb	429
disconnect	120
distance ospf (Router OSPF Config)	1026
distance ospf (Router OSPFv3 Config)	1208
distance rip (Router RIP Config)	1074
distribute-list out (Router OSPF Config)	1027
distribute-list out (Router RIP Config)	1075
distribute-list route-map (Router OSPF Config)	1027
dns-server (DHCP Pool Config)	351
dns-server (IPv6 DHCP Pool Config)	1250
do (Privileged EXEC commands)	63
domain-name	358
domain-name (DHCP Pool Config)	354
domain-name (IPv6 DHCP Pool Config)	1250
domain-name enable	359
dos-control all	829
dos-control firstfrag	830
dos-control icmpfrag	838
dos-control icmpv4	837
dos-control icmpv6	837
dos-control l4port	831
dos-control port-ddisable	832
dos-control sipdip	829
dos-control smacdmac	833
dos-control tcpfinurgpsh	836
dos-control tcpflag	831
dos-control tcpflagseq	834
dos-control tcpfrag	830
dos-control tcpoffset	835
dos-control tcpport	833
dos-control tcpsyn	835
dos-control tcpsynfin	836
dos-control udpport	834
dos-control vlan0tagged-snap	838

dot1as	873
dot1as allowedlostresp	878
dot1as interval announce	875
dot1as interval pdelay	876
dot1as interval sync	875
dot1as pdelay-threshold	877
dot1as priority 1	874
dot1as priority 2	874
dot1as timeout announce	876
dot1as timeout sync	877
dot1x eapolflood	621
dot1x max-reauth-req	623
dot1x max-req	622
dot1x system-auth-control	616
dot1x timeout	628
dot1x user	630
drop	1299
dvlan-tunnel ethertype	561
dying gasp	332
eapol announcements	631
enable	244
enable (Captive Portal Config)	1101
enable (Captive Portal Instance)	1107
enable (Privileged EXEC access)	63
enable (Router OSPF Config)	1013
enable (Router OSPFv3 Config)	1209
enable (Router RIP Config)	1072
enable authentication (Line Config)	133
enable password (Privileged EXEC)	142
encapsulation	927
environment fan control mode	295
environment temprange	296
environment trap	297
erase application	230
erase factory-defaults	252
erase stack-config	252
erase startup-config	252
errdisable recovery cause	853
errdisable recovery cause keepalive	536
errdisable recovery interval	854
erspan-id (ERSPAN Source Session Destination Config)	701
exception core-file	419
exception dump compression	417
exception dump filepath	417
exception dump ftp-server	416

exception dump stack-ip-address add	418
exception dump stack-ip-address protocol	418
exception dump stack-ip-address remove	419
exception dump tftp-server	416
exception protocol	415
exception switch-chip-register	420
exit-overflow-interval (Router OSPF Config)	1028
exit-overflow-interval (Router OSPFv3 Config)	1209
external-lsdb-limit (Router OSPF Config)	1028
external-lsdb-limit (Router OSPFv3 Config)	1209
ezconfig	58
fhrp version vrrp vc3	985
file verify	319
filedescr	257
flowcontrol	602
foreground-color	1117
frequency (IP SLA ICMP Echo Config)	1090
green-mode eee	445
green-mode eee tx-idle-time	445
green-mode eee tx-wake-time	446
green-mode eee-lpi-history max-samples	447
green-mode eee-lpi-history sampling-interval	446
green-mode energy-detect	444
group	1109
hardware-address (DHCP Pool Config)	352
host (DHCP Pool Config)	352
hostname	227
hostroutesaccept (Router RIP Config)	1077
http port (Captive Portal Config)	1102
https port (Captive Portal Config)	1102
icmp-echo	1089
idle-timeout	1114
ignore server-key	187
ignore session-key	187
image verify	320
initiate failover (for stack configuration)	55
interface (Captive Portal Instance)	1115
interface (Global Config) (M4250 series switch)	481
interface (Global Config) (M4350 series switch)	481
interface lag	679
interface loopback	1140
interface vlan	965
ip access-group	1334
ip access-list	1327

ip access-list rename	1328
ip access-list resequence	1328
ip address	915
ip address (ERSPAN Source Session Destination Config)	701
ip address dhcp	916
ip address-conflict-detect run	378
ip arp inspection filter	733
ip arp inspection limit	732
ip arp inspection trust	731
ip arp inspection validate	730
ip arp inspection vlan	730
ip arp inspection vlan	731
ip cpu-priority	62
ip default-gateway	917
ip device tracking (Global Config)	861
ip device tracking maximum (Interface Config)	861
ip device tracking probe	862
ip device tracking probe auto-source fallback	864
ip device tracking probe count	863
ip device tracking probe delay	864
ip device tracking probe interval	863
ip dhcp bootp automatic	361
ip dhcp class	362
ip dhcp conflict logging	362
ip dhcp excluded-address	359
ip dhcp ignore-client-identifier	360
ip dhcp ping packets	360
ip dhcp pool	349
ip dhcp snooping	717
ip dhcp snooping binding	719
ip dhcp snooping database	719
ip dhcp snooping database write-delay (DHCP)	719
ip dhcp snooping database write-delay (DHCPv6)	1260
ip dhcp snooping limit	720
ip dhcp snooping log-invalid	721
ip dhcp snooping trust	722
ip dhcp snooping verify mac-address	718
ip dhcp snooping vlan	718
ip domain list	372
ip domain lookup	371
ip domain name	371
ip domain retry	375
ip domain timeout	375
ip dscp (ERSPAN Source Session Destination Config)	703
ip dvmrp (Global Config)	1376

ip dvmrp (Interface Config)	1377
ip dvmrp metric (Global Config)	1376
ip dvmrp trapflags	1377
ip helper enable	1009
ip helper-address (Global Config)	1005
ip helper-address (Interface Config)	1007
ip host	374
ip http accounting exec	111
ip http authentication	112
ip http port	115
ip http secure-certificate	119
ip http secure-ciphersuite	119
ip http secure-port	118
ip http secure-server	114
ip http secure-session hard-timeout	117
ip http secure-session maxsessions	117
ip http secure-session soft-timeout	118
ip http server	114
ip http session hard-timeout	115
ip http session maxsessions	116
ip http session soft-timeout	116
ip https accounting exec	111
ip https authentication	113
ip icmp echo-reply	1083
ip icmp error-interval	1083
ip igmp	1401
ip igmp header-validation	1402
ip igmp last-member-query-count	1403
ip igmp last-member-query-interval	1403
ip igmp query-interval	1404
ip igmp query-max-response-time	1404
ip igmp robustness	1405
ip igmp startup-query-count	1405
ip igmp startup-query-interval	1406
ip igmp version	1402
ip igmp-proxy	1411
ip igmp-proxy reset-status	1412
ip igmp-proxy unsolicit-rprt-interval	1411
ip irdp	958
ip irdp address	959
ip irdp holdtime	959
ip irdp maxadvertinterval	960
ip irdp minadvertinterval	960
ip irdp multicast	961

ip irdp preference	961
ip load-sharing	918
ip local-proxy-arp	907
ip management	64
ip management source-interface	64
ip mcast boundary	1366
ip mroute	1366
ip mroute static-multicast	1367
ip mtu	926
ip multicast	1368
ip multicast ttl-threshold	1368
ip name server	373
ip name source-interface	373
ip netdirbcast	923
ip ospf area	1036
ip ospf authentication	1037
ip ospf cost	1037
ip ospf database-filter all out	1038
ip ospf dead-interval	1038
ip ospf hello-interval	1039
ip ospf mtu-ignore	1042
ip ospf network	1039
ip ospf prefix-suppression	1040
ip ospf priority	1040
ip ospf retransmit-interval	1041
ip ospf transmit-delay	1041
ip pim	1382
ip pim bsr-border	1383
ip pim bsr-candidat	1384
ip pim dense	1381
ip pim dr-priority	1385
ip pim hello-interval	1383
ip pim join-prune-interval	1386
ip pim rp-address	1387
ip pim rp-candidate	1388
ip pim sparse	1382
ip pim ssm	1389
ip pim-trapflags	1390
ip policy route-map	946
ip prec (ERSPAN Source Session Destination Config)	703
ip prefix-list	924
ip prefix-list description	925
ip proxy-arp	906
ip redirects	1082
ip rip	1073

ip rip authentication	1075
ip rip receive version	1076
ip rip send version	1076
ip route	921
ip route default	922
ip route distance	922
ip route net-prototype	923
ip routing	915
ip scp server enable	330
ip sla	1084
ip sla schedule	1085
ip ssh	85
ip ssh authentication-retries	88
ip ssh port	86
ip ssh pubkey-auth	87
ip ssh server algorithm encryption	89
ip ssh server algorithm hostkey	90
ip ssh server algorithm kex	91
ip ssh server algorithm mac	90
ip ssh server enable	86
ip telnet port	79
ip telnet server enable	79
ip ttl (ERSPAN Source Session Destination Config)	702
ip unnumbered gratuitous-arp accept	919
ip unnumbered loopback	919
ip unreachable	1081
ip verify binding	720
ip verify source	722
ip vrrp (Global Config)	967
ip vrrp (Interface Config)	967
ip vrrp accept-mode	969
ip vrrp authentication	969
ip vrrp ip	968
ip vrrp mode	968
ip vrrp preempt	970
ip vrrp priority	970
ip vrrp timers advertise	971
ip vrrp track interface	972
ip vrrp track ip route	972
ipv6 access-list	1339
ipv6 access-list rename	1340
ipv6 access-list resequence	1340
ipv6 address	1143
ipv6 address autoconfig	1144

ipv6 address dhcp	1144
ipv6 cpu-priority	62
ipv6 dhcp client pd	1245
ipv6 dhcp conflict logging	1246
ipv6 dhcp pool	1248
ipv6 dhcp relay	1247
ipv6 dhcp server	1247
ipv6 dhcp snooping	1259
ipv6 dhcp snooping binding	1261
ipv6 dhcp snooping database	1260
ipv6 dhcp snooping limit	1262
ipv6 dhcp snooping log-invalid	1262
ipv6 dhcp snooping trust	1261
ipv6 dhcp snooping verify mac-address	1260
ipv6 dhcp snooping vlan	1259
ipv6 enable	1142
ipv6 hop-limit	1141
ipv6 host	374
ipv6 icmp error-interval	1160
ipv6 management	70
ipv6 mld last-member-query-count	1444
ipv6 mld last-member-query-interval	1443
ipv6 mld query-interval	1441
ipv6 mld query-max-response-time	1442
ipv6 mld router	1441
ipv6 mld startup-query-count	1443
ipv6 mld startup-query-interval	1442
ipv6 mld version	1444
ipv6 mld-proxy	1450
ipv6 mld-proxy reset-status	1451
ipv6 mld-proxy unsolicit-rprt-interval	1450
ipv6 mroute	1418
ipv6 mtu (M4250 series switch)	1148
ipv6 mtu (M4350 series switch)	1149
ipv6 nd dad attempts	1149
ipv6 nd managed-config-flag	1150
ipv6 nd mtu (M4250 series switch)	1150
ipv6 nd mtu (M4350 series switch)	1151
ipv6 nd ns-interval	1151
ipv6 nd other-config-flag	1152
ipv6 nd prefix	1156
ipv6 nd ra hop-limit unspecified	1154
ipv6 nd rguard attach-policy	1153
ipv6 nd ra-interval	1152
ipv6 nd ra-lifetime	1153

ipv6 nd reachable-time	1154
ipv6 nd router-preference	1155
ipv6 nd suppress-ra	1155
ipv6 neighbor	1157
ipv6 neighbors dynamicrenew	1157
ipv6 nud	1158
ipv6 ospf area	1216
ipv6 ospf cost	1217
ipv6 ospf dead-interval	1217
ipv6 ospf hello-interval	1217
ipv6 ospf link-lsa-suppression	1218
ipv6 ospf mtu-ignore	1218
ipv6 ospf network	1219
ipv6 ospf prefix-suppression	1219
ipv6 ospf priority	1220
ipv6 ospf retransmit-interval	1221
ipv6 ospf transmit-delay	1221
ipv6 pim	1424
ipv6 pim bsr-border	1425
ipv6 pim bsr-candidate	1426
ipv6 pim dense	1423
ipv6 pim dr-priority	1427
ipv6 pim hello-interval	1424
ipv6 pim join-prune-interval	1427
ipv6 pim rp-address	1428
ipv6 pim rp-candidate	1429
ipv6 pim sparse	1423
ipv6 pim ssm	1430
ipv6 policy	1188
ipv6 prefix-list	1190
ipv6 prefix-list description	1189
ipv6 prefix-list renumber	1191
ipv6 redirects	1082
ipv6 route (M4250 series switch)	1145
ipv6 route (M4350 series switch)	1146
ipv6 route distance	1147
ipv6 route net-prototype	1148
ipv6 router ospf	1198
ipv6 traffic-filter	1345
ipv6 unicast-routing	1142
ipv6 unreachable	1159
ipv6 unresolved-traffic	1159
ipv6 verify binding	1264
ipv6 verify source	1263

iscsi aging time	1358
iscsi cos	1359
iscsi cos enable	1360
iscsi enable	1360
iscsi target port	1361
isdnp advertise-v2	845
isdnp enable	846
isdnp holdtime	844
isdnp run	844
isdnp timer	845
keepalive	534
keepalive action	534
keepalive tag	535
key (TACACS Config)	220
keystring (TACACS Config)	220
lacp actor admin key	672
lacp actor admin state	673
lacp actor port priority	674
lacp admin key	671
lacp collector max-delay	672
lacp partner admin key	674
lacp partner admin state individual	675
lacp partner admin state longtimeout	675
lacp partner admin state passive	676
lacp partner port id	676
lacp partner port priority	677
lacp partner system id	677
lacp partner system priority	678
lease (DHCP Pool Config)	353
length	292
line console	76
line ssh	92
line telnet	84
link debounce time	869
link state group action	660
link state group downstream	661
link state group upstream	662
link-flap d-disable	493
link-flap d-disable duration	493
link-flap d-disable max-count	494
lldp med	819
lldp med all	821
lldp med confignotification	819
lldp med confignotification all	822
lldp med faststartrepeatcount	822

lldp med transmit-tlv	820
lldp med transmit-tlv all	821
lldp notification	810
lldp notification-interval	811
lldp portid-subtype	811
lldp receive	807
lldp timers	807
lldp transmit	806
lldp transmit-mgmt	810
lldp transmit-tlv	808
lldp transmit-tlv link-aggregation	809
lldp transmit-tlv max-frame-size	809
lldp transmit-tlv vlan	808
llpf	664
load-interval	910
locale	1115
log-adjacency-changes	1029
logging buffered	297
logging buffered threshold	298
logging buffered wrap	298
logging cli-command	299
logging console	299
logging email	307
logging email from-addr	309
logging email logtime	310
logging email message-type subject	309
logging email message-type to-addr	308
logging email test message-type	311
logging email urgent	308
logging host	300
logging host reconfigure	300
logging host remove	301
logging protocol	301
logging syslog	301
logging syslog port	302
logging syslog source-interface	302
logging syslog usb	302
logging traps	310
logging usb	430
logging usb device-number	431
logging usb overwrite-on-full	431
logging usb stop-on-full	432
login authentication (Line Config)	140
logout	327

mab	624
mab request format attribute 1	625
mac access-group	1317
mac access-list extended	1313
mac access-list extended rename	1314
mac access-list resequence	1314
mac management address	66
mac management type	66
mac-address-table limit	802
mac-address-table notification change	294
macfilter	704
macfilter adddest	705
macfilter adddest all	706
macfilter addsrc	706
macfilter addsrc all	707
mail-server	313
management access-class	109
management access-list	106
mark cos	1300
mark ip-dscp	1301
mark ip-precedence	1301
match any	1288
match class-map	1289
match cos	1290
match destination-address mac	1290
match dstip	1291
match dstip6	1291
match dstl4port	1291
match ethertype	1288
match ip address {access-list-number access-list-name}	948
match ip dscp	1292
match ip precedence	1292
match ip tos	1293
match ip6flowlbl	1293
match ipv6 address	1192
match length	950
match mac-list	951
match metric	953
match metric-type	953
match protocol	1294
match secondary-cos	1290
match secondary-vlan	1296
match source-address mac	1294
match srcip	1295
match srcip6	1295

match srl4port	1295
match tag	954
match vlan	1296
max-bandwidth-down	1112
max-bandwidth-up	1111
maximum-paths (Router OSPF Config)	1031
maximum-paths (Router OSPFv3 Config)	1210
max-input-octets	1112
max-metric router-lsa (OSPFv3 Router Configuration)	1225
max-metric router-lsa (Router OSPF Config)	1046
max-output-octets	1113
max-total-octets	1113
mbuf	422
member (Stack Global Config)	29
memory free low-watermark processor	294
mfa-enable	126
mirror	1299
mmp (Global Config)	885
mmp (Interface Config)	886
mmp periodic state machine	886
mode dot1q-tunnel	562
mode dvlan-tunnel	563
monitor session destination	694
monitor session filter	695
monitor session mode	696
monitor session source	693
monitor session type erspan-source	699
movemanagement (Stack Global Config)	30
mrp	883
msrp (Global Config)	896
msrp (Interface Config)	897
msrp block-avb-traffic-to-cpu	899
msrp boundarypropagate	898
msrp delta-bw	900
msrp max-fan-in-ports	898
msrp srclass-pvid	900
msrp srclassqav class	897
msrp talker-pruning	899
mtu	483
mvr	746
mvr group	747
mvr immediate	749
mvr mode	747
mvr querytime	748

mvr type	749
mvr vlan	748
mvr vlan group	750
mvrp (Global Config)	890
mvrp (Interface Config)	892
mvrp periodic state machine	891
name	1108
netbios-name-server (DHCP Pool Config)	355
netbios-node-type (DHCP Pool Config)	355
network (DHCP Pool Config)	353
network area (Router OSPF Config)	1014
next-server (DHCP Pool Config)	356
no monitor	696
no switchport mode	557
no switchport mode auto	538
no vlan	540
no vlan acceptframe	540
no vlan ingressfilter	541
nsf (Router OSPF Config)	1043
nsf (Router OSPFv3 Config)	1222
nsf (Stack Global Config)	53
nsf helper (Router OSPF Config)	1045
nsf helper (Router OSPFv3 Config)	1224
nsf helper strict-lsa-checking (Router OSPF Config)	1045
nsf helper strict-lsa-checking (Router OSPFv3 Config)	1224
nsf ietf helper disable (Router OSPF Config)	1045
nsf ietf helper disable (Router OSPFv3 Config)	1224
nsf restart-interval (Router OSPF Config)	1044
nsf restart-interval (Router OSPFv3 Config)	1223
ntp (DHCP Pool Config)	358
ntp authenticate	333
ntp authentication-key	334
ntp broadcast client	335
ntp broadcastdelay	336
ntp server	336
ntp source-interface	338
ntp trusted-key	334
openflow controller	232
openflow default-table	233
openflow enable	232
openflow ip-mode	234
openflow passive-mode	234
openflow static-ip	232
openflow variant	235
option (DHCP Pool Config)	356

origin ip address (ERSPAN Source Session Destination Config)	702
passive-interface (Router OSPF Config)	1032
passive-interface (Router OSPFv3 Config)	1211
passive-interface default (Router OSPF Config)	1031
passive-interface default (Router OSPFv3 Config)	1210
password (AAA IAS User Config)	157
password (Line Config)	140
password (Mail Server Config)	314
password (User EXEC)	142
passwords aging	145
passwords history	144
passwords lock-out	145
passwords min-length	144
passwords strength exclude-keyword	150
passwords strength maximum consecutive-characters	147
passwords strength maximum repeated-characters	147
passwords strength minimum character-classes	149
passwords strength minimum lowercase-letters	148
passwords strength minimum numeric-characters	148
passwords strength minimum special-characters	149
passwords strength minimum uppercase-letters	147
passwords strength-check	146
passwords unlock timer	150
passwords unlock timer mode	151
periodic	1350
permit ip host mac host	734
ping	327
ping ipv6	74
ping ipv6 interface	75
poe	1458
poe detection	1458
poe high-power	1459
poe power limit	1460
poe power limit user-defined	1459
poe power management (M4250 series switch)	1461
poe power management (M4350 series switch)	1462
poe priority	1463
poe reset	1464
poe timer schedule	1464
poe traps	1466
poe usagethreshold (M4250 series switch)	1465
poe usagethreshold (M4350 series switch)	1465
police-simple	1302
police-single-rate	1302

police-two-rate	1303
policy-map	1297
policy-map rename	1298
port	188
port (Mail Server Config)	313
port (TACACS Config)	221
port lacpmode	679
port lacpmode enable all	680
port lacptimeout (Global Config)	681
port lacptimeout (Interface Config)	680
port-channel adminmode	681
port-channel auto	665
port-channel auto avb-profile	668
port-channel auto load-balance (M4250 series switch)	666
port-channel auto load-balance (M4350 series switch)	667
port-channel linktrap	682
port-channel load-balance (M4250 series switch)	682
port-channel load-balance (M4350 series switch)	684
port-channel load-balance 0	685
port-channel local-preference	686
port-channel min-links	686
port-channel name	669
port-channel static	679
port-channel system priority	687
port-security	798
port-security aging time	798
port-security mac-address	800
port-security mac-address move	801
port-security mac-address sticky	801
port-security max-dynamic	799
port-security max-static	800
port-security violation shutdown	802
power redundancy	427
preempt (VRRPv3 Config mode)	986
prefix-delegation (IPv6 DHCP Pool Config)	1251
prefix-suppression (Router OSPF Config)	1029
prefix-suppression (Router OSPFv3 Config)	1211
priority (TACACS Config)	221
priority (VRRPv3 Config mode)	987
private-group name	607
private-vlan	567
process cpu threshold	281
protocol	1108
protocol group	547
protocol vlan group	548

protocol vlan group all	548
proxy-ip-address	245
ptp clock e2e-transparent	572
ptp clock-operation	572
ptp ieee version 2.0	590
ptp logging	589
ptp path-trace	589
ptp priority1	574
ptp priority2	574
ptp profile aes67	578
ptp profile aes67 announce	579
ptp profile aes67 delay-request	579
ptp profile aes67 domain	580
ptp profile aes67 sync	581
ptp profile aes-r16-2016	575
ptp profile aes-r16-2016 announce	575
ptp profile aes-r16-2016 delay-request	576
ptp profile aes-r16-2016 domain	577
ptp profile aes-r16-2016 sync	577
ptp profile default	581
ptp profile default announce	582
ptp profile default delay-request	582
ptp profile default domain	583
ptp profile default sync	584
ptp profile default transport	584
ptp profile smpte-2059-2	585
ptp profile smpte-2059-2 announce	585
ptp profile smpte-2059-2 delay-request	586
ptp profile smpte-2059-2 domain	587
ptp profile smpte-2059-2 sync	588
ptp profile smpte-2059-2 transport	588
ptp source	573
quit	331
radius accounting mode	189
radius server attribute 30	191
radius server attribute 31	192
radius server attribute 32	192
radius server attribute 4	189
radius server attribute 44	194
radius server attribute 95	190
radius server dead-criteria	205
radius server deadtime	206
radius server host {ipaddr ipv6address hostname}	194
radius server host link local	197

radius server key	199
radius server load-balance	203
radius server msgauth	200
radius server primary	201
radius server retransmit	201
radius server timeout	204
radius server vsa send	204
radius source-interface	202
radius-auth-server	1110
random-detect exponential-weighting-constant	1278
random-detect queue-parms	1278
redirect	1110
redirect	1300
redirect-url	1111
redistribute (Router OSPF Config)	1030
redistribute (Router OSPFv3 Config)	1212
redistribute (Router RIP Config)	1078
redistribute ospf (Router RIP Config)	1078
relay agent information remote-id circuit-id (DHCP Class Config)	363
release dhcp	920
reload (for stack configuration)	35
reload (Privileged EXEC)	331
reload configuration	331
remark	1319
remark	735
remote-span	551
renew dhcp	920
rgb-led brightness	486
rgb-led color	486
rgb-led mode	485
rmon alarm	454
rmon collection history	458
rmon event	457
rmon hcalarm	455
route-map	947
router ospf	1013
router rip	1072
router-id (Router OSPF Config)	1030
router-id (Router OSPFv3 Config)	1213
routing	914
script apply	224
script delete	224
script dhcpclient-config delete	226
script dhcpclient-config list	225
script dhcpclient-config show	226

script list	224
script show	225
script validate	225
sdm prefer	441
security (Mail Server Config)	313
separator-color	1118
serial baudrate (Line Config)	77
serial timeout (Line Config)	77
server-key	188
service dhcp	361
service dhcpv6	1245
service-policy	1304
serviceport ip	65
serviceport ipv6 address	71
serviceport ipv6 enable	71
serviceport ipv6 gateway	72
serviceport ipv6 neighbor	72
serviceport protocol	65
serviceport protocol dhcp	65
session start	424
session stop	425
session-limit (Line Config)	81
session-timeout (Captive Portal Instance)	1114
session-timeout (Line Config)	82
set clibanner	228
set garp timer join	608
set garp timer leave	609
set garp timer leaveall	609
set gmrp adminmode	613
set gmrp interfacemode	613
set gvrp adminmode	611
set gvrp interfacemode	611
set igmp	755
set igmp exclude-mrouter-intf	762
set igmp fast-leave	757
set igmp fast-leave auto-assignment	757
set igmp flood-report	762
set igmp groupmembership-interval	758
set igmp header-validation	764
set igmp interfacemode	756
set igmp maxresponse	759
set igmp mcrptreptime	760
set igmp mrouter	761
set igmp mrouter interface	761

set igmp proxy-querier	777
set igmp querier	773
set igmp querier election participate	775
set igmp querier query-interval	774
set igmp querier timer expiry	774
set igmp querier version	775
set igmp report-suppression	763
set igmp-plus (Global Config)	765
set igmp-plus (VLAN Config)	765
set interface	954
set ip default next-hop	956
set ip next-hop	955
set ip precedence	956
set ipv6 default next-hop	1195
set ipv6 next-hop	1194
set ipv6 precedence	1196
set mld	779
set mld exclude-mrouter-intf	785
set mld fast-leave	780
set mld groupmembership-interval	781
set mld interfacemode	780
set mld maxresponse	782
set mld mcrtrexpiretime	783
set mld mrouter	784
set mld mrouter interface	784
set mld proxy-querier	796
set mld querier	792
set mld querier election participate	794
set mld querier query-interval	793
set mld querier timer expiry	794
set mld-plus (Global Config)	786
set mld-plus (VLAN Config)	786
set prompt	227
set slot disable (for stack configuration)	32
set slot power (for stack configuration)	33
set sup-console	77
sflow poller	435
sflow receiver	432
sflow receiver owner	433
sflow sampler	434
sflow source-interface	436
show "command" begin "string"	255
show "command" exclude "string"	254
show "command" include "string"	253
show "command" include "string" exclude "string2"	254

show "command" section "string"	255
show "command" section "string" "string2"	255
show "command" section "string" include "string2"	256
show aaa ias-users	158
show access-lists interface	1338
show access-lists vlan	1339
show accounting	160
show accounting methods	160
show accounting update	161
show application	230
show application files	231
show arp	912
show arp access-list	738
show arp brief	913
show arp switch (Address Resolution Protocol commands)	913
show arp switch (System Information and Statistics commands)	258
show arp-guard attack history	744
show arp-guard statistics	742
show arp-guard summary	741
show authentication	637
show authentication authentication-history	637
show authentication clients	648
show authentication interface	638
show authentication methods	640
show authentication statistics	641
show authorization methods	132
show auto-copy-sw (for stack firmware synchronization)	52
show auto-dos	841
show autoinstall	253
show auto-vlan	555
show auto-voip	1356
show auto-voip oui-table	1357
show bonjour	871
show bootpdhcprelay	1003
show bootvar	257
show captive-portal	1104
show captive-portal client status	1122
show captive-portal client status	1123
show captive-portal configuration	1119
show captive-portal configuration client status	1125
show captive-portal configuration interface	1119
show captive-portal configuration locales	1121
show captive-portal configuration status	1120
show captive-portal interface capability	1127

show captive-portal interface client status	1124
show captive-portal interface configuration status	1126
show captive-portal status	1105
show captive-portal trapflags	1106
show captive-portal user	1137
show capture packets	382
show checkpoint statistics (for stack configuration)	55
show class-map	1306
show classofservice dot1p-mapping	1281
show classofservice ip-dscp-mapping	1281
show classofservice trust	1282
show clibanner	227
show clock	348
show clock detail	348
show cloud-managed	247
show crypto certificate all	102
show crypto certificate mycertificate	103
show crypto dhparam	104
show crypto key mypubkey	104
show crypto key pubkey-chain ssh	105
show dampening interface	1071
show debugging	415
show dhcp client vendor-id-option	717
show dhcp l2relay agent-option vlan	714
show dhcp l2relay all	712
show dhcp l2relay circuit-id vlan	712
show dhcp l2relay interface	713
show dhcp l2relay remote-id vlan	713
show dhcp l2relay stats interface	714
show dhcp l2relay vlan	715
show dhcp lease	927
show diffserv	1307
show diffserv service	1310
show diffserv service brief	1311
show domain-name	161
show dos-control	839
show dot1as interface	879
show dot1as statistics	882
show dot1as summary	878
show dot1q-tunnel	563
show dot1x	643
show dot1x users	649
show dvlan-tunnel	564
show dying-gasp status	332
show environment	259

show errdisable recovery	854
show eventlog	258
show exception	421
show fiber-ports optics	270
show fiber-ports optics-diag	276
show fiber-ports optics-eeprom	277
show fiber-ports optics-info	278
show flowcontrol	602
show forwardingdb agetime	842
show garp	610
show gmrp configuration	614
show green-mode	447
show green-mode eee-lpi-history	451
show gvrp configuration	612
show hardware	259
show hosts	376
show igmpsnooping	766
show igmpsnooping fast-leave	768
show igmpsnooping group	769
show igmpsnooping mrouter interface	770
show igmpsnooping mrouter vlan	771
show igmpsnooping proxy-querier	778
show igmpsnooping querier	776
show igmpsnooping ssm	771
show interface	261
show interface dampening	1071
show interface debounce	870
show interface ethernet	264
show interface ethernet switchport	269
show interface lag	263
show interface loopback	1140
show interface switchport	559
show interfaces cos-queue	1282
show interfaces description	273
show interfaces diag	274
show interfaces random-detect	1283
show interfaces status	271
show interfaces status err-disabled	855
show interfaces switchport	560
show interfaces switchport (for a group ID)	605
show interfaces switchport trunk	538
show interfaces traffic	272
show ip access-lists	1335
show ip address-conflict	378

show ip arp inspection	735
show ip arp inspection interfaces	738
show ip arp inspection statistics	736
show ip brief	928
show ip device tracking all	865
show ip device tracking interface	866
show ip device tracking ip	867
show ip device tracking mac	868
show ip dhcp binding	367
show ip dhcp class configuration	370
show ip dhcp client statistics	929
show ip dhcp conflict	370
show ip dhcp global configuration	367
show ip dhcp pool configuration	368
show ip dhcp server statistics	369
show ip dhcp snooping	723
show ip dhcp snooping binding	723
show ip dhcp snooping database	724
show ip dhcp snooping interfaces	725
show ip dhcp snooping statistics	726
show ip dvmrp	1378
show ip dvmrp interface	1378
show ip dvmrp neighbor	1379
show ip dvmrp nexthop	1380
show ip dvmrp prune	1380
show ip dvmrp route	1380
show ip helper statistics	1011
show ip helper-address	1010
show ip http	119
show ip igmp	1406
show ip igmp groups	1407
show ip igmp interface	1408
show ip igmp interface membership	1409
show ip igmp interface stats	1410
show ip igmp-proxy	1412
show ip igmp-proxy groups	1414
show ip igmp-proxy groups detail	1415
show ip igmp-proxy interface	1413
show ip interface	931
show ip interface brief	934
show ip irdp	962
show ip load-sharing	934
show ip management	67
show ip mcast	1369
show ip mcast boundary	1369

show ip mcast interface	1370
show ip mfc	1390
show ip mroute	1371
show ip mroute group	1372
show ip mroute source	1372
show ip mroute static	1373
show ip mroute static-multicast	1374
show ip ospf	1048
show ip ospf abr	1052
show ip ospf area	1053
show ip ospf asbr	1054
show ip ospf database	1055
show ip ospf database database-summary	1056
show ip ospf interface	1057
show ip ospf interface brief	1059
show ip ospf interface stats	1059
show ip ospf lsa-group	1061
show ip ospf neighbor	1062
show ip ospf range	1065
show ip ospf statistics	1065
show ip ospf stub table	1067
show ip ospf traffic	1067
show ip ospf virtual-link	1069
show ip ospf virtual-link brief	1069
show ip pim	1391
show ip pim bsr-router	1396
show ip pim interface	1393
show ip pim neighbor	1395
show ip pim rp mapping	1398
show ip pim rp-hash	1397
show ip pim ssm	1393
show ip pim statistics	1399
show ip policy	957
show ip prefix-list	944
show ip protocols	935
show ip rip	1079
show ip rip interface	1080
show ip rip interface brief	1080
show ip route	936
show ip route ecmp-groups	938
show ip route hw-failure	938
show ip route kernel	939
show ip route net-prototype	939
show ip route preferences	943

show ip route summary	940
show ip route track-table	1096
show ip sla configuration	1094
show ip sla statistics	1095
show ip source binding	729
show ip ssh	92
show ip stats	945
show ip verify	727
show ip verify source	728
show ip vlan	966
show ip vrrp	973
show ip vrrp interface	974
show ip vrrp interface brief	975
show ip vrrp interface stats	975
show ipv6 access-lists	1346
show ipv6 brief	1160
show ipv6 dhcp	1252
show ipv6 dhcp binding	1254
show ipv6 dhcp conflict	1255
show ipv6 dhcp interface	1253
show ipv6 dhcp pool	1255
show ipv6 dhcp snooping	1264
show ipv6 dhcp snooping binding	1265
show ipv6 dhcp snooping database	1266
show ipv6 dhcp snooping interfaces	1267
show ipv6 dhcp snooping statistics	1267
show ipv6 dhcp statistics	1252
show ipv6 interface (M4250 series switch)	1162
show ipv6 interface (M4350 series switch)	1165
show ipv6 interface vlan	1168
show ipv6 mld groups	1445
show ipv6 mld interface	1447
show ipv6 mld traffic	1448
show ipv6 mld-proxy	1451
show ipv6 mld-proxy groups	1453
show ipv6 mld-proxy groups detail	1454
show ipv6 mld-proxy interface	1452
show ipv6 mroute	1419
show ipv6 mroute group	1420
show ipv6 mroute source	1420
show ipv6 mroute static	1421
show ipv6 nd raguard policy	1168
show ipv6 neighbors (M4250 series switch)	1169
show ipv6 neighbors (M4350 series switch)	1169
show ipv6 ospf	1227

show ipv6 ospf abr	1230
show ipv6 ospf area	1231
show ipv6 ospf asbr	1232
show ipv6 ospf database	1232
show ipv6 ospf database database-summary	1233
show ipv6 ospf interface	1234
show ipv6 ospf interface brief	1235
show ipv6 ospf interface stats	1236
show ipv6 ospf lsa-group	1237
show ipv6 ospf max-metric	1239
show ipv6 ospf neighbor	1239
show ipv6 ospf range	1241
show ipv6 ospf statistics	1242
show ipv6 ospf stub table	1243
show ipv6 ospf virtual-link	1243
show ipv6 ospf virtual-link brief	1244
show ipv6 pim	1431
show ipv6 pim bsr-router	1435
show ipv6 pim interface	1433
show ipv6 pim neighbor	1434
show ipv6 pim rp mapping	1437
show ipv6 pim rp-hash	1437
show ipv6 pim ssm	1432
show ipv6 pim statistics	1439
show ipv6 prefix-list	1186
show ipv6 protocols	1185
show ipv6 route (M4250 series switch)	1170
show ipv6 route (M4350 series switch)	1172
show ipv6 route 6to4	1176
show ipv6 route ecmp-groups	1174
show ipv6 route hw-failure	1175
show ipv6 route kernel	1176
show ipv6 route net-prototype	1176
show ipv6 route preferences	1177
show ipv6 route summary	1177
show ipv6 route track-table	1097
show ipv6 snooping counters	1180
show ipv6 source binding	1271
show ipv6 traffic	1181
show ipv6 verify	1269
show ipv6 verify source	1270
show ipv6 vlan	1181
show iscsi	1362
show iscsi sessions	1363

show isdp	847
show isdp entry	849
show isdp interface	848
show isdp neighbors	850
show isdp traffic	851
show keepalive	536
show keepalive statistics	537
show lacp actor	687
show lacp partner	688
show link state group	662
show link state group detail	663
show link-flap d-disable	494
show lldp	812
show lldp interface	813
show lldp local-device	817
show lldp local-device detail	818
show lldp med	823
show lldp med interface	823
show lldp med local-device detail	824
show lldp med remote-device	826
show lldp med remote-device detail	827
show lldp remote-device	814
show lldp remote-device detail	816
show lldp statistics	813
show llpf interface	664
show logging	303
show logging buffered	305
show logging email config	311
show logging email statistics	312
show logging hosts	305
show logging traplogs	306
show login session	121
show login session long	121
show mab	642
show mac access-lists	1320
show mac-address-table gmrp	615
show mac-address-table igmpsnooping	772
show mac-address-table mldsnooping	791
show mac-address-table multicast	842
show mac-address-table notification change	173
show mac-address-table static	707
show mac-address-table staticfiltering	708
show mac-address-table stats	843
show mac-addr-table	279
show mail-server config	314

Fully Managed Switches M4250 and M4350 Series

show management access-class	110
show management access-list	109
show mbuf	422
show mbuf total	423
show mfa	127
show mfa log	127
show mldsnooping	787
show mldsnooping mrouter interface	788
show mldsnooping mrouter vlan	789
show mldsnooping proxy-querier	797
show mldsnooping querier	795
show mldsnooping ssm entries	789
show mldsnooping ssm groups	791
show mldsnooping ssm stats	790
show mmrp	887
show mmrp statistics	888
show monitor session	697
show mrp	884
show msg-queue	424
show msrp	901
show msrp interface bandwidth	902
show msrp reservations	902
show msrp statistics	904
show msrp stream	903
show mvr	750
show mvr interface	752
show mvr members	751
show mvr traffic	753
show mvrp	892
show mvrp statistics	894
show nsf (for stack configuration)	54
show ntp	338
show ntp associations	343
show ntp authentication-keys	339
show ntp information	344
show ntp packets	342
show ntp servers	340
show ntp status	341
show openflow	235
show openflow configured controller	236
show openflow installed flows	237
show openflow installed groups	239
show openflow table-status	241
show passwords configuration	151

show passwords result	152
show platform vpd	261
show poe	1466
show poe port configuration	1467
show poe port info	1468
show policy-map	1307
show policy-map interface	1311
show port	487
show port advertise	489
show port description	490
show port protocol	549
show port status	491
show port-channel	689
show port-channel auto	668
show port-channel brief	688
show port-channel counters	691
show port-channel global-load-balance	690
show port-channel system priority	691
show port-security	803
show port-security dynamic	804
show port-security static	805
show port-security violation	805
show power	428
show power redundancy	428
show private-group	607
show process app-list	282
show process cpu (M4250 series switch)	283
show process cpu (M4350 series switch)	284
show process memory	282
show process proc-list	286
show ptp boundary-clock	593
show ptp interface	592
show ptp parent	595
show ptp path-trace	596
show ptp statistics	596
show ptp summary	598
show ptp time-properties	599
show radius	206
show radius accounting	209
show radius accounting statistics	211
show radius server dynamic-author	215
show radius server dynamic-author statistics	215
show radius servers	207
show radius source-interface	212
show radius statistics	213

show RGB LED configuration	491
show rmon alarm alarms	459
show rmon collection history	460
show rmon events	462
show rmon hcalarms	468
show rmon history	463
show rmon log	465
show rmon statistics interfaces	466
show route-map	958
show routing heap summary	945
show running-config	286
show running-config interface	288
show sdm prefer	442
show serial	78
show service-policy	1312
show serviceport	68
show serviceport ipv6 dhcp statistics	1256
show serviceport ipv6 neighbors	73
show sflow agent	437
show sflow pollers	438
show sflow receivers	438
show sflow samplers	440
show sflow source-interface	440
show slot	36
show snmp	178
show snmp engineID	178
show snmp filters	179
show snmp group	180
show snmp user	180
show snmp views	181
show snmp-server	177
show spanning-tree	515
show spanning-tree active	517
show spanning-tree backbonefast	520
show spanning-tree brief	521
show spanning-tree interface	521
show spanning-tree mst detailed	524
show spanning-tree mst port detailed	524
show spanning-tree mst port summary	528
show spanning-tree mst port summary active	530
show spanning-tree mst summary	531
show spanning-tree summary	531
show spanning-tree uplinkfast	532
show spanning-tree vlan	532

show stack-hashmode	37
show stack-port	43
show stack-port counters	43
show stack-port diag	44
show stack-port stack-path	49
show stack-status	38
show startup-config backup-config factory-defaults	288
show stats flow-based	477
show stats group	475
show storm-control	659
show supported cardtype (for stack configuration)	39
show supported switchtype (for stack configuration)	42
show sw reset	426
show switch	39
show switchport protected	605
show sysinfo	292
show tacacs	222
show tacacs source-interface	222
show telnet	84
show telnetcon	85
show terminal length	293
show time-range	1351
show track	1097
show trapflags (M4250 series switch)	181
show trapflags (M4350 series switch)	182
show udd	858
show usb device	429
show users	137
show users accounts	138
show users login-history	139
show users login-history [long]	139
show users long	137
show version	260
show vlan	552
show vlan association mac	555
show vlan association oui	556
show vlan association subnet	555
show vlan internal usage	553
show vlan port	554
show vlan remote-span	698
show voice vlan	570
show vrrp	976
show vrrp	991
show vrrp brief	982
show vrrp brief	997

show vrrp statistics	983
show vrrp statistics	998
shutdown (Interface Config)	484
shutdown (VRRPv3 Config mode)	989
shutdown all	484
slot (for stack configuration)	32
snmp trap link-status	176
snmp trap link-status all	176
snmp trap mac-notification change	177
snmp-server	162
snmp-server community	163
snmp-server community-group	164
snmp-server enable traps	169
snmp-server enable traps captive-portal	1104
snmp-server enable traps captive-portal	172
snmp-server enable traps linkmode	170
snmp-server enable traps mac-notification change	172
snmp-server enable traps multiusers	171
snmp-server enable traps stpmode	171
snmp-server enable traps violation	169
snmp-server engineid local	162
snmp-server filter	173
snmp-server group	167
snmp-server host	165
snmp-server port	174
snmp-server trapsend	175
snmp-server user	168
snmp-server v3-host	166
snmp-server view	174
snmptrap source-interface	175
source interface (ERSPAN Source Session Config)	699
spanning-tree	495
spanning-tree auto-edge	495
spanning-tree backbonefast	496
spanning-tree bpdudfilter	497
spanning-tree bpdudfilter default	497
spanning-tree bpdudflood	498
spanning-tree bpduguard	498
spanning-tree bpdumigrationcheck	499
spanning-tree configuration name	499
spanning-tree configuration revision	500
spanning-tree cost	500
spanning-tree edgeport	501
spanning-tree forward-time	501

spanning-tree guard	502
spanning-tree max-age	502
spanning-tree max-hops	503
spanning-tree mode	503
spanning-tree mst	504
spanning-tree mst instance	505
spanning-tree mst priority	506
spanning-tree mst vlan	506
spanning-tree port mode	507
spanning-tree port mode all	508
spanning-tree port-priority	508
spanning-tree tcnguard	509
spanning-tree transmit	509
spanning-tree uplinkfast	510
spanning-tree vlan	511
spanning-tree vlan cost	511
spanning-tree vlan forward-time	512
spanning-tree vlan hello-time	512
spanning-tree vlan max-age	513
spanning-tree vlan port-priority	515
spanning-tree vlan priority	514
spanning-tree vlan root	514
speed	485
split-horizon (Router RIP Config)	1077
sshcon maxsessions	87
sshcon timeout	88
stack	29
stack-port	43
stack-status sample-mode	35
standby	31
stats flow-based (Global Config)	472
stats flow-based (Interface Config)	475
stats flow-based reporting	473
stats group (Global Config)	471
stats group (Interface Config)	474
storm-control broadcast	651
storm-control broadcast action	651
storm-control broadcast level	652
storm-control broadcast rate	653
storm-control multicast	653
storm-control multicast action	654
storm-control multicast level	655
storm-control multicast rate	655
storm-control unicast	656
storm-control unicast action	657

storm-control unicast level	657
storm-control unicast rate	658
sw reset	425
switch priority	30
switch renumber	30
switchport access vlan	559
switchport mode	556
switchport mode auto	538
switchport mode private-vlan	566
switchport private-group	606
switchport private-vlan	565
switchport protected (Global Config)	603
switchport protected (Interface Config)	604
switchport trunk allowed vlan	557
switchport trunk native vlan	558
tacacs-server host	217
tacacs-server key	218
tacacs-server keystring	218
tacacs-server source-interface	219
tacacs-server timeout	219
telnet	80
telnetcon maxsessions	82
telnetcon timeout	83
terminal length	293
threshold (IP SLA ICMP Echo Config)	1092
timeout (IP SLA ICMP Echo Config)	1091
timeout (TACACS Config)	221
time-range	1349
timers advertize (VRRPv3 Config mode)	988
timers pacing flood (Router OSPF Config)	1032
timers pacing lsa-group (Router OSPF Config)	1033
timers pacing lsa-group (Router OSPFv3 Config)	1213
timers spf (Router OSPF Config)	1034
timers throttle spf (Router OSPFv3 Config)	1214
traceroute	320
track interface (VRRPv3 Config mode)	989
track ip sla	1086
traffic-shape	1280
transport input telnet (Line Config)	80
transport output telnet (Line Config)	81
trapflags (Captive Portal Config)	1103
trapflags (Router OSPF Config)	1034
trapflags (Router OSPFv3 Config)	1215
trunk-hashmode	34

udld enable (Global Config)	856
udld enable (Interface Config)	857
udld message time	857
udld port	858
udld reset	858
udld timeout interval	857
unmount usb	430
update bootcode	257
url	246
user (Captive Portal Config)	1128
user {user-id} group (Captive Portal Config)	1136
user group (Captive Portal Config)	1135
user group moveusers (Captive Portal Config)	1136
user group name (Captive Portal Config)	1136
user idle-timeout (Captive Portal Config)	1131
user max-bandwidth-down (Captive Portal Config)	1132
user max-bandwidth-up (Captive Portal Config)	1132
user max-input-octets (Captive Portal Config)	1133
user max-output-octets (Captive Portal Config)	1134
user max-total-octets (Captive Portal Config)	1134
user name (Captive Portal Config)	1129
user password (Captive Portal Config)	1129
user password encrypted (Captive Portal Config)	1130
user session-timeout (Captive Portal Config)	1130
user-logout	1116
username (Global Config)	133
username (Mail Server Config)	314
username name nopassword	135
username sshkey file	136
username unlock	136
verification	1109
vlan	539
vlan acceptframe	540
vlan association mac	551
vlan association oui	552
vlan association subnet	550
vlan database	539
vlan ingressfilter	540
vlan internal allocation	541
vlan makestatic	541
vlan name	542
vlan participation	542
vlan participation all	543
vlan port acceptframe all	544
vlan port ingressfilter all	544

vlan port priority all	601
vlan port pvid all	545
vlan port tagging all	545
vlan priority	601
vlan protocol group	546
vlan protocol group add protocol	547
vlan protocol group name	546
vlan pvid	549
vlan routing	963
vlan tagging	550
voice vlan (Global Config)	568
voice vlan (Interface Config)	569
voice vlan auth	569
voice vlan data priority	570
voice vlan dscp	570
vrf (IP SLA ICMP Echo Config)	1093
vrrp address-family	985
write core	420
write memory	331