NETGEAR®

M5300, M6100, and M7100 Series ProSAFE Managed Switches

CLI Command Reference Manual

Software Version 11.0.0

April 2015
202-11526-02



350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for selecting NETGEAR products.

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

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

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

Contact your Internet service provider for technical support.

Compliance

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

See the regulatory compliance document before connecting the power supply.

Trademarks

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

Revision History

Publication Part Number	Publish Date	Comments
202-11526-01	March 2015	Added the following chapter and section: • *Chapter 5, Stacking Commands* • *Switch Port Commands* Added the following main commands: • *ip management* • *snmp-server port* and *show snmp-server* • *show fiber-ports optics-diag* • *exception dump ftp-server*, *exception dump compression*, *exception dump stack-ip-address protocol*, *exception dump stack-ip-address add*, and *exception dump stack-ip-address remove* • *exception nmi* • *show msg-queue* • *sw reset* and *show sw reset* • *peer detection interval* • *system-mac* • *system-priority* • *debug vpc peer-link data-message* • *set igmp header-validation* • *show igmpsnooping querier* • *set mld proxy-querier* and *show mldsnooping proxy-querier* Made changes and corrections to other commands.
202-11457-02	September 2014	Corrected the syntax of the *{deny | permit} (IPv6)* command. Added a note to all debug commands.
202-11457-01	August 2014	Initial publication of this manual.

Contents

Chapter 1 About the NETGEAR Managed Switch Software

Scope 9
Product Concept 9

Chapter 2 Using the Command-Line Interface

Command Syntax 11
Command Conventions 11
Common Parameter Values 12
unit/slot/port Naming Convention 13
Using the No Form of a Command 14
Executing Show Commands 14
CLI Output Filtering 14

Chapter 3 NETGEAR Managed Switch Software Modules

Command Modes 17
Command Completion and Abbreviation 22
CLI Error Messages 22
CLI Line-Editing Conventions 23
Using CLI Help 24
Accessing the CLI 25

Chapter 4 Chassis Commands

General Chassis Commands 27
Backplane Port Commands 36
Chassis Firmware Synchronization Commands 37
Nonstop Forwarding Commands for Chassis Configuration 39

Chapter 5 Stacking Commands

Dedicated Port Stacking Commands 44
Stack Port Commands 55
Stack Firmware Synchronization Commands 61
Nonstop Forwarding Commands for Stack Configuration 63

Chapter 6 Management Commands

Configure the Switch Management CPU 69
CPU Queue Commands 71

Network Interface Commands 72
Console Port Access Commands 78
Telnet Commands 81
Secure Shell Commands 86
Management Security Commands 88
Management Access Control List Commands 89
Hypertext Transfer Protocol Commands 94
Access Commands 101
User Account Commands 103
Per-Command Authorization 107
Exec Authorization 107
SNMP Commands 133
RADIUS Commands 145
TACACS+ Commands 160
Configuration Scripting Commands 165
Prelogin Banner, System Prompt, and Host Name Commands 167

Chapter 7 Utility Commands

AutoInstall Commands 171
CLI Output Filtering Commands 175
Dual Image Commands 177
System Information and Statistics Commands 178
Switch Services Commands 207
Logging Commands 209
Email Alerting and Mail Server Commands 217
System Utility and Clear Commands 223
Simple Network Time Protocol Commands 235
Time Zone Commands 241
DHCP Server Commands 245
DNS Client Commands 258
IP Address Conflict Commands 263
Serviceability Packet Tracing Commands 264
Support Mode Commands 302
Cable Test Command 305
Power Management Commands 306
USB commands 310
sFlow Commands 311
Switch Database Management Template Commands 318
Green Ethernet Commands 322
Remote Monitoring Commands 331
Statistics Application Commands 347

Chapter 8 Switching Commands

Port Configuration Commands 357
Spanning Tree Protocol Commands 364
VLAN Commands 395

Switch Port Commands 408
Double VLAN Commands 413
Private VLAN Commands 416
Voice VLAN Commands 418
Provisioning (IEEE 802.1p) Commands 422
Asymmetric Flow Control 422
Protected Ports Commands 424
Private Group Commands 426
GARP Commands 428
GVRP Commands 430
GMRP Commands 432
Port-Based Network Access Control Commands 434
802.1X Supplicant Commands 456
Storm-Control Commands 460
Link Local Protocol Filtering Commands 467
MRP Commands 468
MMRP Commands 469
MVRP Commands 473
Port-Channel/LAG (802.3ad) Commands 476
VPC Commands 495
Port Mirroring Commands 509
Static MAC Filtering Commands 512
DHCP L2 Relay Agent Commands 516
DHCP Client Commands 523
DHCP Snooping Configuration Commands 525
Dynamic ARP Inspection Commands 535
MVR Commands 542
IGMP Snooping Configuration Commands 549
IGMP Snooping Querier Commands 558
MLD Snooping Commands 563
MLD Snooping Querier Commands 571
Port Security Commands 576
LLDP (802.1AB) Commands 581
LLDP-MED Commands 589
Denial of Service Commands 597
MAC Database Commands 607
ISDP Commands 609
UniDirectional Link Detection Commands 617
Link Debounce Commands 620

Chapter 9 Data Center Commands

Data Center Bridging Exchange Protocol Commands 624
Enhanced Transmission Selection and Traffic Class Group 631
FIP Snooping Commands 636
Priority-Based Flow Control Commands 655

Chapter 10 Routing Commands

Address Resolution Protocol Commands 661
IP Routing Commands. 667
Routing Policy Commands 691
Router Discovery Protocol Commands 715
Virtual LAN Routing Commands 719
Virtual Router Redundancy Protocol Commands 722
DHCP and BootP Relay Commands. 731
IP Helper Commands. 733
Open Shortest Path First Commands 741
General OSPF Commands 741
OSPF Interface Commands 762
IP Event Dampening Commands. 768
OSPF Graceful Restart Commands 770
OSPFv2 Stub Router Commands 773
OSPF Show Commands 775
Routing Information Protocol Commands 796
ICMP Throttling Commands. 804

Chapter 11 Captive Portal Commands

Captive Portal Global Commands 808
Captive Portal Configuration Commands 813
Captive Portal Status Commands 822
Captive Portal Client Connection Commands. 824
Captive Portal Interface Commands. 827
Captive Portal Local User Commands 829
Captive Portal User Group Commands. 836

Chapter 12 Border Gateway Protocol Commands

BGP Commands 839
Routing Policy Commands 916

Chapter 13 IPv6 Commands

IPv6 Management Commands 923
Tunnel Interface Commands 929
Loopback Interface Commands. 931
IPv6 Routing Commands 932
OSPFv3 Commands 967
Global OSPFv3 Commands 967
OSPFv3 Interface Commands. 983
OSPFv3 Graceful Restart Commands 988
OSPFv3 Stub Router Commands 992
OSPFv3 Show Commands. 993
DHCPv6 Commands 1010
DHCPv6 Snooping Configuration Commands. 1023

Chapter 14 Quality of Service Commands

Class of Service Commands 1035
Differentiated Services Commands 1043
DiffServ Class Commands 1044
DiffServ Policy Commands 1053
DiffServ Service Commands 1060
DiffServ Show Commands 1061
MAC Access Control List Commands 1067
IP Access Control List Commands 1073
IPv6 Access Control List Commands 1087
Time Range Commands for Time-Based ACLs 1094
Auto-Voice over IP Commands 1097
iSCSI Optimization Commands 1102

Chapter 15 IP Multicast Commands

Multicast Commands 1110
DVMRP Commands 1117
PIM Commands 1122
Internet Group Message Protocol Commands 1137
IGMP Proxy Commands 1145

Chapter 16 IPv6 Multicast Commands

IPv6 Multicast Forwarder 1153
IPv6 PIM Commands 1157
IPv6 MLD Commands 1171
IPv6 MLD-Proxy Commands 1177

Chapter 17 Power over Ethernet Commands

About PoE 1184
PoE Commands 1185

Chapter 18 NETGEAR Managed Switch Software Log Messages

Core 1196
Utilities 1198
Management 1201
Switching 1204
QoS 1212
Routing/IPv6 Routing 1213
Multicast 1215
Chassis 1220
Technologies 1221
O/S Support 1223

Command List

About the NETGEAR Managed Switch Software

1

The NETGEAR Managed Switch software has two purposes:

- Assist attached hardware in switching frames, based on Layer 2, 3, or 4 information contained in the frames.
- Provide a complete device management portfolio to the network administrator.

This chapter contains the following sections:

- *Scope*
- *Product Concept*

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

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

Scope

NETGEAR Managed Switch software encompasses both hardware and software support. The software is partitioned to run in the following processors:

- **CPU**. This code runs the networking device management portfolio and controls the overall networking device hardware. It also assists in frame forwarding, as needed and specified. This code is designed to run on multiple platforms with minimal changes from platform to platform.
- **Networking device processor**. This code does the majority of the packet switching, usually at wire speed. This code is platform dependent, and substantial changes might exist across products.

Product Concept

Fast Ethernet and Gigabit Ethernet switching continues to evolve from high-end backbone applications to desktop switching applications. The price of the technology continues to decline, while performance and feature sets continue to improve. Devices that are capable of switching Layers 2, 3, and 4 are increasingly in demand. NETGEAR Managed Switch software provides a flexible solution to these ever-increasing needs.

The exact functionality provided by each networking device on which the NETGEAR Managed Switch software base runs varies depending upon the platform and requirements of the NETGEAR Managed Switch software.

NETGEAR Managed Switch software includes a set of comprehensive management functions for managing both NETGEAR Managed Switch software and the network. You can manage the NETGEAR Managed Switch software by using one of the following three methods:

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

Using the Command-Line Interface

2

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*
- *unit/slot/port Naming Convention*
- *Using the No Form of a Command*
- *Executing Show Commands*
- *CLI Output Filtering*

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 network** and **clear vlan**, do not require parameters. Other commands, such as **network parms**, 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 **network parms** command syntax:

Format	network parms *ipaddr netmask* [gateway]

- **network parms** is the command name.
- *ipaddr* and *netmask* are parameters and represent required values that you must enter after you type the command keywords.
- [**gateway**] is an optional keyword, so you are not required to enter a value in place of the keyword.

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 shows.

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
italic font	*value* 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.

Table 1. Parameter Conventions (continued)

Symbol	Example	Description
`| 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 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 *n* 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.)
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.
Interface or *unit/slot/port*	Valid slot and port number separated by a forward slash. For example, 0/1 represents slot number 0 and port number 1.
Logical Interface	Represents a logical slot and port number. This is applicable in the case of a port-channel (LAG). You can use the logical unit/slot/port 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.

unit/slot/port Naming Convention

NETGEAR Managed Switch software references physical entities such as cards and ports by using a *unit/slot/port* naming convention. The NETGEAR Managed Switch software also uses this convention to identify certain logical entities, such as Port-Channel interfaces.

The slot number has two uses. In the case of physical ports, it identifies the card containing the ports. In the case of logical and CPU ports it also identifies the type of interface or port.

Table 3. Type of Slots

Slot Type	Description
Physical slot numbers	Physical slot numbers begin with zero, and are allocated up to the maximum number of physical slots.
Logical slot numbers	Logical slots immediately follow physical slots and identify port-channel (LAG) or router interfaces. The value of logical slot numbers depend on the type of logical interface and can vary from platform to platform.
CPU slot numbers	The CPU slots immediately follow the logical slots.

The port identifies the specific physical port or logical interface being managed on a given slot.

Table 4. Type of Ports

Port Type	Description
Physical Ports	The physical ports for each slot are numbered sequentially starting from one. For example, port 1 on slot 0 (an internal port) for a switch is 1/0/1, port 2 is 1/0/2, port 3 is 1/0/3, and so on.
Logical Interfaces	Port-channel or Link Aggregation Group (LAG) interfaces are logical interfaces that are only used for bridging functions. VLAN routing interfaces are only used for routing functions. Loopback interfaces are logical interfaces that are always up. Tunnel interfaces are logical point-to-point links that carry encapsulated packets.
CPU ports	CPU ports are handled by the driver as one or more physical entities located on physical slots.

Note: In the CLI, loopback and tunnel interfaces do not use the *unit/slot/port* format. To specify a loopback interface, you use the loopback ID. To specify a tunnel interface, you use the tunnel ID.

Using the 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.

Executing 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. Previously, show commands could be issued only in User EXEC or Privileged EXEC modes.

CLI Output Filtering

Many CLI show commands include considerable content to display to the user. 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 NETGEAR Managed 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 specificed 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 175.

NETGEAR Managed Switch Software Modules

3

NETGEAR Managed Switch software consists of flexible modules that can be applied in various combinations to develop advanced Layer 2/3/4+ products. The commands and command modes available on your switch depend on the installed modules. Additionally, for some **show** commands, the output fields might change based on the modules included in the NETGEAR Managed Switch software.

The NETGEAR Managed Switch software suite includes the following modules:

- Switching (Layer 2)
- Routing (Layer 3)
- IPv6 routing
- Multicast
- BGP-4
- Quality of Service
- Management (CLI, Web UI, and SNMP)
- IPv6 Management—Allows management of the NETGEAR Managed Switch device through an IPv6 through an IPv6 address without requiring the IPv6 Routing package in the system. The management address can be associated with the network port (front-panel switch ports), a routine interface (port or VLAN) and the Service port.
- Metro
- Chassis management
- Data Center
- Secure Management

Command Modes

The CLI groups commands into modes according to the command function. Each of the command modes supports specific NETGEAR Managed Switch software 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.

Note: The command modes available on your switch depend on the software modules that are installed. For example, a switch that does not support BGPv4 does not have the BGPv4 Router Command Mode.

Table 5. 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	`Switch (Vlan)#`	Groups all the VLAN commands.
Interface Config	`Switch (Interface unit/slot/port)#`	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 Loopback id)#`	
	`Switch (Interface Tunnel id)#`	
	`Switch (Interface unit/slot/port (startrange)-unit/slot/port (endrange)#`	Use this mode to manage the operation of a range of interfaces. For example the prompt may display as follows: `Switch (Interface 1/0/1-1/0/4) #`
	`Switch (Interface lag lag-intf-num)#`	Enters LAG Interface configuration mode for the specified LAG.
	`Switch (Interface vlan vlan-id)#`	Enters VLAN routing interface configuration mode for the specified VLAN ID.

Table 5. CLI Command Modes (continued)

Command Mode	Prompt	Mode Description
Line Console	`Switch (config-line)#`	Contains commands to configure outbound telnet settings and console interface settings, as well as to configure console login/enable authentication.
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-class-map)#`	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)#`	Contains the OSPF configuration commands.
Router OSPFv3 Config	`Switch (Config rtr)#`	Contains the OSPFv3 configuration commands.
Router RIP Config	`Switch (Config-router)#`	Contains the RIP configuration commands.
BGP Router Config	`Switch (Config-router)#`	Contains the BGP4 configuration commands.
Route Map Config	`Switch (config-route-map)#`	Contains the route map configuration commands.
IPv6 Address Family Config	`Switch (Config-router-af)#`	Contains the IPv6 address family configuration commands.
Peer Template Config	`(Config-rtr-tmplt)#`	Contains the BGP peer template configuration commands.
MAC Access-list Config	`Switch (Config-mac-access-list)#`	Allows you to create a MAC Access-List and to enter the mode containing MAC Access-List configuration commands.

Table 5. CLI Command Modes (continued)

Command Mode	Prompt	Mode Description
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 dhcp6-pool)#`	Contains the DHCPv6 server IPv6 address pool configuration commands.
Chassis Global Config Mode	`Switch (Config chassis)#`	Allows you to access the Chassis 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.
Support Mode	`Switch (Support)#`	Allows access to the support commands, which should only be used by the manufacturer's technical support personnel as improper use could cause unexpected system behavior and/or invalidate product warranty.

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

Table 6. CLI Mode Access and Exit

Command Mode	Access Method	Exit or Access 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	From the Privileged EXEC mode, enter **`vlan database`**.	To exit to the Privileged EXEC mode, enter **`exit`**, or press **`Ctrl-Z.`**

Table 6. CLI Mode Access and Exit (continued)

Command Mode	Access Method	Exit or Access Previous Mode
Interface Config	From the Global Config mode, enter: **interface** *unit/slot/port*	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** *loopback id*	
	From the Global Config mode, enter: **interface** *tunnel id*	
	From the Global Config mode, enter: **interface** *unit/slot/port*(startrange)-*unit/slot/port*(endrange)	
	From the Global Config mode, enter: **interface lag** *lag-intf-num*	
	From the Global Config mode, enter: **interface vlan** *vlan-id*	
Line Console	From the Global Config mode, enter **line console**.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
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** *name*.	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** *address*.	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**.	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**.	To exit to the Policy Map mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
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 1045 for more information.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.

Table 6. CLI Mode Access and Exit (continued)

Command Mode	Access Method	Exit or Access Previous Mode
VPC	From Global Config mode, enter **vpc**.	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 1045 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**.	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**.	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**.
BGP Router Config	From the Global Config mode, enter **router bgp** *asnumber*.	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** *map-tag*.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
IPv6 Address Family Config	From the BGP Router Config mode, enter **address-family ipv6**.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
Peer Template Config	From the BGP Router Config mode, enter **template peer** *name* to create a BGP peer template and enter Peer Template Configuration mode.	o 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** *name*.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.
TACACS Config	From the Global Config mode, enter **tacacs-server host** *ip-addr*, where *ip-addr* 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** *pool-name*.	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 **ip dhcpv6 pool** *pool-name*.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter **Ctrl-Z**.

Table 6. CLI Mode Access and Exit (continued)

Command Mode	Access Method	Exit or Access Previous Mode
Chassis Global Config Mode	From the Global Config mode, enter **chassis**.	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**.
Support Mode	From the Privileged EXEC mode, enter **support**. **Note:** The **support** command is available only if the **techsupport enable** command has been issued.	To exit to the Privileged EXEC mode, enter **exit**, or press **Ctrl-Z**.

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 7. 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 8. 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.
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.

Using 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
```

Accessing 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 *Network Interface Commands* on page 72.

Chassis Commands

4

This chapter describes the chassis commands available in the NETGEAR Managed Switch CLI.

Note: These commands apply to the M6100 series switches only.

The Chassis Commands chapter includes the following sections:

- *General Chassis Commands*
- *Backplane Port Commands*
- *Chassis Firmware Synchronization Commands*
- *Nonstop Forwarding Commands for Chassis Configuration*

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.

General Chassis Commands

This section describes the commands you use to configure the chassis.

chassis

This command sets the mode to Chassis Global Config.

Format	`chassis`
Mode	Chassis Global Config

chassis-status sample-mode

This command set the global status management mode.

Format	`chassis-status sample-mode [cumulative | history [max-samples <100-500>]]`
Mode	Chassis Global Config

Parameter	Description
cumulative	Tracks the sum of received time stamp offsets cumulatively.
history	Tracks the history of received timestamps.
max-samples	As an option for the *history* parameter, the maximum number of samples to keep. The valid range is from 100 to 500.

member (Chassis Global Config)

This command configures a blade. The *unit* is the identifier of the blade that you want to add or remove from the chassis. The *switchindex* is the index into the database of the supported blade types, indicating the type of the blade that is being preconfigured. The blade index is a 32-bit integer. You execute this command on the management blade.

Format	`member` *unit switchindex*
Mode	Chassis Global Config

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

no member

This command removes a blade from the chassis. The *unit* is the identifier of the blade to be removed from the chassis. You execute this command on the primary management blade.

Format	`no member` *unit*
Mode	Chassis Global Config

movemanagement (Chassis Global Config)

This command moves the management functionality from one blade to the other. The *fromunit* is the identifier of the current management blade. The *tounit* is the identifier of the new management blade. Upon execution, the entire chassis (including all interfaces in the chassis) is unconfigured and reconfigured with the configuration on the new management blade. After the reload is complete, you must perform all chassis management capabilities on the new management blade. To preserve the current configuration across a management blade move, execute the **`copy system:running-config nvram:startup-config`** privileged EXEC command or **`save`** privileged EXEC command before you perform the management blade move. A management blade move causes all routes and layer 2 addresses to be lost. You execute this command is executed on the management blade. The system prompts you to confirm the management blade move.

Note: You can only configure the blade in slot 1 or slot 2 as a management blade.

Format	`movemanagement` *fromunit tounit*
Mode	Chassis Global Config

slot (for chassis configuration)

This command configures a slot in the system. The *unit/slot* is the slot identifier of the slot. The *cardindex* is the index into the database of the supported card types, indicating the type of the card being preconfigured in the specified slot. The card index is a 32-bit integer. If a card is currently present in the slot that is unconfigured, the configured information will be deleted and the slot will be reconfigured with default information for the card.

Format	`slot` *unit/slot cardindex*
Mode	Global Config

Note: Card index can be obtained by executing show supported cardtype command in User EXEC mode.

no slot

This command removes configured information from an existing slot in the system.

Format	`no slot` *`unit/slot cardindex`*
Mode	Global Config

Note: Card index can be obtained by executing show supported cardtype command in User EXEC mode.

set slot disable (for chassis configuration)

This command configures the administrative mode of the slot(s). If you specify **`all`**, the command is applied to all slots, otherwise the command is applied to the slot identified by *`unit/slot`*.

If a card or other module is present in the slot, this administrative mode will effectively be applied to the contents of the slot. If the slot is empty, this administrative mode will be 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.

Format	`set slot disable [`*`unit/slot`*`] | all]`
Mode	Global Config

no set slot disable

This command unconfigures the administrative mode of the slot or slots. If you specify **`all`**, the command removes the configuration from all slots, otherwise the configuration is removed from the slot identified by *`unit/slot`*.

If a card or other module is present in the slot, this administrative mode removes the configuration from the contents of the slot. If the slot is empty, this 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	`no set slot disable [`*`unit/slot`*`] | all]`
Mode	Global Config

set slot power (for chassis configuration)

This command configures the power mode of the slot(s) and allows power to be supplied to a card located in the slot. If you specify **`all`**, the command is applied to all slots, otherwise the command is applied to the slot identified by *`unit/slot`*.

Use this command when installing or removing cards. If a card or other module is present in this 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.

Format	`set slot power [unit/slot] | all]`
Mode	Global Config

no set slot power

This command unconfigures the power mode of the slot or slots and prohibits power from being supplied to a card located in the slot. If you specify **all**, the command prohibits power to all slots, otherwise the command prohibits power to the slot identified by *unit/slot*.

Use this command when installing or removing cards. If a card or other module is present in this 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	`no set slot power [unit/slot] | all]`
Mode	Global Config

reload (for chassis configuration)

This command resets the entire chassis or the identified *blade*. The *blade* is the blade identifier. The system prompts you to confirm that you want to reset the chassis or blade.

Format	`reload [blade]`
Mode	Global Config

show supported cardtype (for chassis configuration)

This commands displays information about all card types or specific card types supported in the system.

Format	`show supported cardtype [cardindex]`
Mode	User EXEC

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

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

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

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 chassis

This command displays chassis status information about all blades in the chassis or, if you specify the *unit* value, about a single blade. For blades that would normally be allowed to join the chassis but do not have a matching chassis template ID, the blade status is shown as STM Mismatch.

Format	`show chassis [unit]`
Mode	Privileged EXEC

Term	Definition
Unit	The unit identifier assigned to the blade.

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

Term	Definition
Management Role	Indicates whether the blade is the supervisor blade, a member blade, or an operational backup blade, or whether the status is unassigned.
Preconfigured Model Identifier	The model identifier of a preconfigured blade that is ready to join the chassis. The Model Identifier is a 32-character field that is assigned by the device manufacturer to identify the device.
Plugged-In Model ID	The model identifier of the blade in the chassis. The Model Identifier is a 32-character field that is assigned by the device manufacturer to identify the device.
Switch Status	The chassis status. Possible values for this state are: OK, Unsupported, Code Mismatch, SDM Mismatch, Config Mismatch, or Not Present. A mismatch indicates that a blade is running a different software version, has a different SDM template, or has a different configuration from the management blade. The SDM Mismatch status indicates that the blade joined the chassis, but has a different SDM template than the management blade. This status is temporary; the blade automatically reloads using the template of the chassis manager. If a chassis firmware synchronization operation is in progress, the status is shown as Updating Code.
Code Version	The detected version of code on this blade.

Command example:

```
(NETGEAR Switch) #show chassis

        Management    Plugged-in    Serial         Switch         Version      Admin    PoE
Unit    Role          Model ID      Number         Status         Code         State    Card
------  ----------    ------------  -------------  -------------  -----------  -------  --------
1       Primary       XCM8944-PoE+  33J1245WF0021  OK             5.26.23.31   Enable   XCM89P
2       Oper Standby  XCM8948-uPoE  33J1245WF0022  CodeMismatch   5.26.23.31   Enable   XCM89UP
3       Chassis Mbr   XCM8924X      33J1245WF0023  NoPwr          5.26.23.31   Enable   N/A
```

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

Term	Definition
Unit	The unit number of the blade.
Management Status	Indicates whether the blade is the supervisor blade, the backup blade, a member blade, or unassigned.
Hardware Management Preference	The hardware management preference of the blade. The hardware management preference can be disabled or unassigned.
Admin Management Preference	The administrative management preference value that is assigned to the blade. This preference value indicates how likely the blade is to be selected as the primary management blade.
Admin State	Administrative state of the blade.
Power State	Power state of the blade.
Switch Type	The 32-bit numeric blade type.
Plugged-in Model Identifier	The model identifier of the blade in the chassis. The Model Identifier is a 32-character field that is assigned by the device manufacturer to identify the device.
Switch Status	The blade status. Possible values are OK, Unsupported, Code Mismatch, Config Mismatch, SDM Mismatch, or Not Present. A mismatch indicates that the blade is running a different version of the code, SDM template, or configuration than the management blade. The SDM Mismatch status indicates that the blade is part of the chassis, but is running a different SDM template than the management blade. A mismatch status is temporary; the blade automatically reloads using the template that is running on the management blade. If a chassis firmware synchronization operation is in progress, the status is shown as Updating Code.
Switch Description	The blade description.
Detected Code in Flash	The version of code that is currently stored in FLASH memory on the blade. This code executes after the blade is reset. If the blade is not present and the data is from preconfiguration, then the code version is “None”.
POE D-Card description	The description of the PoE daughter card that is plugged into the blade.
POE D-Card PoE firmware version	The firmware version that is running on the PoE controller of the daughter card that is plugged into the blade.

Term	Definition
CPLD Version	The version of CPLD firmware that is running on the blade.
SFS Last Attempt Status	The chassis firmware synchronization status in the last attempt for the blade.
Serial Number	The serial number for the blade.
Up Time	The system up time.

Command example:

```
(NETGEAR Switch) #show chassis 1

Switch.......................... 1
Management Status................ Management Switch
Hardware Management Preference.... Unassigned
Admin Management Preference...... 15
Admin State...................... Enable
Power State...................... Enable
Switch Type...................... 0x4320004
Preconfigured Model Identifier.... XCM8948
Plugged-in Model Identifier...... XCM8948
Switch Status.................... OK
Switch Description............... XCM8948 ProSafe 48-port Gigabit blade
Detected Code in Flash........... 5.26.23.31
CPLD version ............ ........ 0x01
POE D-card Description........... XCM89UP ProSafe UPoE daughter card
POE D-card PoE FW version.......   1.0
SFS Last Attempt Status.......... None
Serial Number.................... 33J1245WF0021
Up Time.......................... 4 days 21 hrs 52 mins 51 secs
```

Command example:

```
(NETGEAR Switch) #show chassis 2

Switch.......................... 2
Management Status................ Standby Management unit
Hardware Management Preference.... Unassigned
Admin Management Preference...... 14
Admin State...................... Enable
Power State...................... Enable
Switch Type...................... 0x5320005
Preconfigured Model Identifier.... XCM8948
Plugged-in Model Identifier...... XCM8948
Switch Status.................... OK
Switch Description............... XCM8948 ProSafe 48-port Gigabit blade
Detected Code in Flash........... 5.26.23.31
```

```
CPLD version ..... ........ 0x01
POE D-card Description..... XCM89P ProSafe PoE+ daughter card
POE D-card PoE FW version.......   1.0
SFS Last Attempt Status..... None
Serial Number..... 33J1245WF0022
Up Time..... 4 days 21 hrs 52 mins 41 secs
```

Command example:

```
(NETGEAR Switch) #show chassis 3

Switch..... 3
Management Status..... Chassis Member
Hardware Management Preference.... Unassigned
Admin Management Preference..... Disabled
Admin State..... Enable
Power State..... Enable
Switch Type..... 0x4320004
Preconfigured Model Identifier.... XCM8948
Plugged-in Model Identifier..... XCM8948
Switch Status..... OK
Switch Description..... XCM8948 ProSafe 48-port Gigabit blade
Detected Code in Flash..... 5.26.23.31
CPLD version ..... ........ 0x01
POE D-card Description..... Not Installed
POE D-card PoE FW version.....   NA
SFS Last Attempt Status..... None
Serial Number..... 2X61295V00008
Up Time..... 4 days 21 hrs 56 mins 25 secs
```

show chassis watchdog

This command shows the internal watchdog timer on the switch, which reboots the switch if the CPU becomes stuck or does not respond.

Format	`show chassis watchdog`
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch)# show chassis watchdog
Slot  Watchdog counter
1     0
2     1
3     0
```

show chassis-status

Every two seconds, a blade broadcasts heartbeat messages. A state table on the supervisor and each blade tracks every unit in the chassis. The table maintains a running history of the heartbeat messages, current observed interval, and the minimum, maximum, and average observed times between heartbeat messages. Sequence numbers in the discovery messaged determine loss.

Format	`chassis-status unit [`*`unit`*` | all] [clear]`
Mode	User EXEC

Command example:

```
(NETGEAR Switch) #show chassis-status 1

Chassis Unit 1 Status
Unit    Current    Average    Min     Max    Dropped
 1      2000       2000       2000    2000   0
 2      2000       2100       2000    2500   0
 3      2000       2100       2000    2200   0
```

show supported switchtype (for chassis configuration)

This commands displays information about all supported switch types or a specific switch type.

Format	`show supported switchtype [`*`switchindex`*`]`
Mode	User EXEC Privileged EXEC

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

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

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

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

Backplane Port Commands

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

show backplane-port

This command displays summary backplane-port information for all interfaces.

Format	`show backplane-port`
Mode	Privileged EXEC

For each Interface:

Term	Definition
Unit	The blade number.
Interface	The blade and port numbers.
Link Status	Status of the link.
Link Speed	Speed (Gbps) of the blade port link.

show backplane-port counters

This command displays summary data counter information for all interfaces.

Format	`show backplane-port counters`
Mode	Privileged EXEC

Term	Definition
Unit	The slot number.
Interface	The slot and port numbers.
Tx Data Rate	Trashing data rate in megabits per second on the backplane port.
Tx Error Rate	Platform-specific number of transmit errors per second.

Term	Definition
Tx Total Errors	Platform-specific number of total transmit errors since power-up.
Rx Data Rate	Receive data rate in megabits per second on the backplane port.
Rx Error Rate	Platform-specific number of receive errors per second.
Rx Total Errors	Platform-specific number of total receive errors since power-up.
Link Flaps	The number of times this backplane port transitioned to the down state.

show backplane-port diag

This command shows backplane port diagnostics for each port and is only intended for Field Application Engineers (FAEs) and developers. An FAE will advise on the necessity to run this command and capture this information.

Format	`show backplane-port diag [<1-3> | all] [verbose]`
Mode	Privileged EXEC

show backplane-port packet-path

This command displays the route a packet will take to reach the destination.

Format	`show backplane-port packet-path {1-3 | all}`
Mode	Privileged EXEC

show backplane

This command displays the backplane model ID, FAPGA version, and serial number.

Format	`show backplane`
Mode	Privileged EXEC

Chassis Firmware Synchronization Commands

Chassis Firmware Synchronization (CFS) provides the ability to automatically synchronize firmware for all chassis members. If a blade joins the chassis and its firmware version is different from the version running on the chassis manager, the CFS feature can either upgrade or downgrade the firmware on the mismatched chassis member. There is no attempt to synchronize the blade to the latest firmware in the chassis.

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

Use this command to enable the Chassis Firmware Synchronization feature on the chassis.

Default	Disabled
Format	`boot auto-copy-sw`
Mode	Privileged Exec

no boot auto-copy-sw

Use this command to disable the Chassis Firmware Synchronization feature on the chassis.

Format	`no boot auto-copy-sw`
Mode	Privileged Exec

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

Use this command to enable the sending of SNMP traps that are related to the Chassis Firmware Synchronization feature.

Default	Enabled
Format	`boot auto-copy-sw trap`
Mode	Privileged Exec

no boot auto-copy-sw trap

Use this command to disable the sending of traps that are related to the Chassis Firmware Synchronization feature.

Format	`no boot auto-copy-sw trap`
Mode	Privileged Exec

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

Use this command to allow the chassis manager to downgrade the firmware version on the chassis member if the firmware version on the manager is older than the firmware version on the chassis member.

Default	Enabled
Format	`boot auto-copy-sw allow-downgrade`
Mode	Privileged Exec

no boot auto-copy-sw allow-downgrade

Use this command to prevent the chassis manager from downgrading the firmware version of a chassis member.

Format	`no boot auto-copy-sw allow-downgrade`
Mode	Privileged Exec

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

Use this command to display chassis firmware synchronization configuration status information.

Format	`show auto-copy-sw`
Mode	Privileged Exec

Term	Definition
Synchronization	Shows whether the CFS feature is enabled.
SNMP Trap Status	Shows whether the chassis will send traps for CFS events.
Allow Downgrade	Shows wether the manager is permitted to downgrade the firmware version of a chassis member.

Nonstop Forwarding Commands for Chassis Configuration

Note: Nonstop forwarding (NSF) is enabled by default on the chassis. You cannot disable NSF on the chassis.

A switch can be described in terms of three semi-independent functions called the forwarding plane, the control plane, and the management plane. The forwarding plane forwards data packets. The forwarding plane is implemented in hardware. The control plane is the set of protocols that determine how the forwarding plane should forward packets, deciding which data packets are allowed to be forwarded and where they should go. Application software on the management blade acts as the control plane. The management plane is application software running on the management blade that provides interfaces allowing a network administrator to configure and monitor the device.

NSF allows the forwarding plane of chassis blades 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 blade. A nonstop forwarding failover can also be manually initiated using the **`initiate failover`** command. Traffic flows that enter and exit the

chassis through physical ports on a blade other than the management blade continue with at most subsecond interruption when the management blade fails.

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

When a nonstop forwarding failover occurs, the control plane on the backup blade starts from a partially-initialized state and applies the checkpointed state information. While the control plane is initializing, the chassis cannot react to external changes, such as network topology changes. Once the control plane is fully operational on the new management blade, the control plane ensures that the hardware state is updated as necessary. Control plane failover time depends on the size of the chassis, 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. NETGEAR Managed Switch software uses three techniques to prevent traffic from being rerouted:

- A protocol may distribute a part of its control plane to chassis blades 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 may 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 768).
- A protocol may simply restart after the failover if neighbors react slowly enough that they will not normally detect the outage. The IP multicast routing protocols are a good example of this behavior.

To take full advantage of nonstop forwarding, layer 2 connections to neighbors should be via port channels that span two or more chassis slots, and layer 3 routes should be ECMP routes with next hops via physical ports on two or more slots. The hardware can quickly move traffic flows from port channel members or ECMP paths on a failed blade to a surviving blade.

show nsf (for chassis configuration)

This command displays global and per-blade information on NSF configuration on the chassis.

Format	`show nsf`
Mode	Privileged Exec

Parameter	Description
NSF Administrative Status	Whether nonstop forwarding is administratively enabled or disabled. Default: Enabled
NSF Operational Status	Indicates whether NSF is enabled on the chassis.
Last Startup Reason	The type of activation that caused the software to start the last time: “Power-On” means that the blade rebooted. This could have been caused by a power cycle or an administrative “Reload” command. “Administrative Move” means that the administrator issued the **movemanagement** command for the stand-by manager to take over. “Warm-Auto-Restart” means that the primary management blade restarted due to 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 close together.
Time Since Last Restart	Time since the current management blade became the active management blade.
Restart in progress	Whether a restart is in progress.
Warm Restart Ready	Whether the system is ready to perform a nonstop forwarding failover from the management blade to the backup blade.
Copy of Running Configuration to Backup Unit: Status	Whether the running configuration on the backup blade includes all changes made on the management blade.
Time Since Last Copy	When the running configuration was last copied from the management blade to the backup blade.
Time Until Next Copy	The number of seconds until the running configuration will be copied to the backup blade. This line only appears when the running configuration on the backup blade is Stale.
Per Unit Status Parameters	
NSF Support	Whether a blade supports NSF.

initiate failover (for chassis configuration)

This command forces the backup blade to take over as the management blade and perform a warm restart of the chassis. On a warm restart, the backup blade becomes the management blade without clearing its hardware tables. (On a cold restart, hardware tables are cleared.) Applications apply checkpointed data from the former management blade. The original management blade reboots.

If the system is not ready for a warm restart, for example, because no backup blade was elected or one or more members of the chassis do not support nonstop forwarding, the command fails with a warning message.

The **movemanagement** command (see *movemanagement (Chassis Global Config)* on page 28) also transfers control from the current management blade; however, the hardware is cleared and all blades reinitialize.

Format	`initiate failover`
Mode	Chassis Global Config Mode

show checkpoint statistics (for chassis configuration)

This command displays general information about the checkpoint service operation.

Format	`show checkpoint statistics`
Mode	Privileged Exec

Parameter	Description
Messages Checkpointed	Number of checkpoint messages transmitted to the backup blade. Range: Integer. Default: 0
Bytes Checkpointed	Number of bytes transmitted to the backup blade. Range: Integer. Default: 0
Time Since Counters Cleared	Number of days, hours, minutes and seconds since the counters were reset to zero. The counters are cleared when a blade becomes manager and with a support command. Range: Time Stamp. Default: 0d00:00:00
Checkpoint Message Rate	Average number of checkpoint messages per second. The average is computed over the time period since the counters were cleared. Range: Integer. Default: 0
Last 10-second Message Rate	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

clear checkpoint statistics (for chassis configuration)

This command clears all checkpoint statistics to their initial values.

Format	`clear checkpoint statistics`
Mode	Privileged Exec

Stacking Commands

5

This chapter describes the stacking commands available in the NETGEAR Managed Switch CLI.

Note: Stacking commands are supported on the M5300 series switches only.

This chapter contains the following sections:

- *Dedicated Port Stacking Commands*
- *Stack Port Commands*
- *Stack Firmware Synchronization 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 unit that controls the stack.

Dedicated Port Stacking Commands

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

stack

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

Default	None
Format	`stack`
Mode	Global Config

member (Stack Global Config)

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` *`unit switchindex`*
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` *`unit`*
Mode	Stack Global Config

switch priority

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	`switch` *`unit`* `priority` *`value`*
Mode	Global Config

switch renumber

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	`switch` *`oldunit`* `renumber` *`newunit`*
Mode	Global Config

movemanagement (Stack Global Config)

Use this command to move the Primary Management Unit 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 66.

Default	None
Format	`movemanagement` *`fromunit tounit`*
Mode	Stack Global Config

standby

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	`standby` *`unit number`*
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	`no standby`
Mode	Stack Global Config

slot (for stack configuration)

Use this command to configure a slot in the system. The *`unit/slot`* is the slot identifier of 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	`slot` *`unit/slot cardindex`*
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	`no slot` *`unit/slot cardindex`*
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)

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

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	`set slot disable [`*`unit/slot`*` | all]`
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 **all**, 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*.

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	`no set slot disable [`*`unit/slot`*` | all]`
Mode	Global Config

set slot power (for stack configuration)

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

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	`set slot power [unit/slot | all]`
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 **all**, the command prohibits power to all slots, otherwise the command prohibits power to the slot that is identified by *unit/slot*.

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	`no set slot power [unit/slot | all]`
Mode	Global Config

reload (for stack configuration)

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 [unit]`
Mode	User EXEC

stack-status sample-mode

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` *`number`*`]`
Mode	Stack Global Config

Command example:

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

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

Format	`show slot [unit/slot]`
Mode	User EXEC Privileged EXEC

Term	Definition
Slot	The slot identifier in the unit/slot format.
Slot Status	The slot is empty, full, or has encountered an error
Admin State	The slot administrative mode is enabled or disabled.
Power State	The slot power mode is enabled or disabled.
Configured Card Model Identifier	The model identifier of the card preconfigured in the slot. The model identifier is a 32-character field used to identify a card.
Pluggable	Cards are pluggable or non-pluggable in the slot.
Power Down	Indicates whether the slot can be powered down.

If you supply a value for *unit/slot*, 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-status

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)

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

Format	`show supported cardtype [cardindex]`
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.

Term	Definition
Model Identifier	The model identifier for the supported card type.
Card Description	The description for the supported card type.

show switch

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 [`*`unit`*`]`
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.
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.......................  0x2320002
Preconfigured Model Identifier....  M5300-28G3
Plugged-in Model Identifier.......  M5300-28G3
Switch Status.....................  OK
```

```
Switch Description.............. M5300-28G3 ProSafe 24-port Gigabit L3 with 10 Gigabit
Stacking
Detected Code in Flash............ 11.0.0.2
CPLD version..................... 0x5
SFS Last Attempt Status........... None
Serial Number..................... 2WD12456F0039
Up Time.......................... 0 days 19 hrs 33 mins 1 secs
```

show supported switchtype (for stack configuration)

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

Format	`show supported switchtype [`*`switchindex`*`]`
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

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

Default	stack
Format	stack-port *unit/slot/port* {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

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

                ------------TX------------------ ------------RX-------------- -------
                Data       Error                Data     Error
                Rate       Rate        Total    Rate     Rate       Total    Link
Unit Interface  (Mb/s)     (Errors/s)  Errors   (Mb/s)   (Errors/s) Errors   Flaps
---- ---------- ---------- ----------- -------- -------- ---------- -------- -------
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

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.
- **all**. The output displays for all units in the stack.

Format	show stack-port diag [*number* | 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
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

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.
- **all**. 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 [*source-unit* | all] [*destination-unit*]
Mode	Privileged EXEC

Stack Firmware Synchronization 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)

Use this command to enable stack firmware synchronization.

Default	Disabled
Format	boot auto-copy-sw
Mode	Privileged EXEC

no boot auto-copy-sw

Use this command to disable stack firmware synchronization.

Format	`no boot auto-copy-sw`
Mode	Privileged EXEC

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

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

Default	Enabled
Format	`boot auto-copy-sw trap`
Mode	Privileged EXEC

no boot auto-copy-sw trap

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

Format	`no boot auto-copy-sw trap`
Mode	Privileged EXEC

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

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	`boot auto-copy-sw allow-downgrade`
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

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

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

Format	`show auto-copy-sw`
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 wether 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 768).
- 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)

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 master 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	`nsf`
Mode	Stack Global Config

no nsf

Use this command to disable nonstop forwarding on the stack.

Format	`no nsf`
Mode	Stack Global Config

show nsf (for stack configuration)

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

Format	`show nsf`
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 **`movemanagement`** 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.
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 (*Per Unit Status Parameter)*	Indicates whether a unit supports NSF.

initiate failover (for stack configuration)

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 45) also transfers control from the current management unit. However, the hardware is cleared and all units reinitialize.

Default	None
Format	`initiate failover`
Mode	Stack Global Config

show checkpoint statistics (for stack configuration)

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

Format	`show checkpoint statistics`
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)

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

Format	`clear checkpoint statistics`
Mode	Privileged EXEC

Management Commands

6

This chapter describes the management commands available in the NETGEAR Managed Switch CLI.

The Management Commands chapter contains the following sections:

- *Configure the Switch Management CPU*
- *CPU Queue Commands*
- *Network Interface 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*

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 is applicable to all NETGEAR M6100 series managed switches and 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

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 should vary in a 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.
Do you want to assign it (password length should vary in a range of 8 - 64 characters)
(Y/N/Q)?  y
```

```
Enter new password:********
Confirm new password:********
Assigning an IP address to your switch management

Current IP Address Configuration
--------------------------------

Management VLAN ID: 1
IP Address Assignment Mode: None
IP Address: 0.0.0.0
Subnet mask: 0.0.0.0
Default Router IP: 0.0.0.0
Routing Mode: Disable

IP address is not assigned. What do you want to do?
C - Configure IP address manually.
D - Assign IP address for the switch using DHCP mode(current IP address will be
lost).
N - Do nothing and go to the next question.
Q - Quit.
? - Help.
(C/D/N/Q/?)? c

IP Address: 10.10.10.1
Network mask: 255.255.255.0
Gateway: 10.10.10.10
Do you want routing to be enabled (Y/N)?y

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)y

the System Name:testchassis
the System Location:testlab
the System Contact:Bud Lightyear
Do you want to apply and save the changes (Y/N)?  y

Could not set the Default Router IP address!
```

```
Config file 'startup-config' created successfully .

The configuration changes have been applied and saved.
Please enter 'show running-config' to see the final configuration.

Thanks for using EzConfig!
```

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

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	`ip cpu-priority` *`ip-address`*
Mode	Privileged EXEC

no ip cpu-priority

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

Format	`no ip cpu-priority` *`ip-address`*
Mode	Privileged EXEC

ipv6 cpu-priority

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	`ip cpu-priority` *`ipv6-address`*
Mode	Privileged EXEC

no ipv6 cpu-priority

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

Format	`no ip cpu-priority` *`ipv6-address`*
Mode	Privileged EXEC

Network Interface Commands

This section describes the commands you use to configure a logical interface for management access. To configure the management VLAN, see *network mgmt_vlan* on page 395.

enable (Privileged EXEC access)

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)

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

Format	`do` *`Priv Exec Mode Command`*
Mode	• Global Config • Interface Config • VLAN Config • 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

Use this command to specify the source IP address for all applications (syslog, SNMP client, and so on).

Default	`vlan 1`
Format	`ip management [serviceport | vlan number | port unit/slot/port | loopback number]`
Mode	User EXEC

no ip management

Use this command to specify the IP address of the management VLAN (VLAN 1) as the source IP address for all applications (syslog, SNMP client, and so on).

Format	`no ip management [serviceport | vlan number | port unit/slot/port | loopback number]`
Mode	User EXEC

serviceport ip

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	`serviceport ip {ipaddr netmask [gateway] | none}`
Mode	Privileged EXEC

serviceport protocol

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	`serviceport protocol {none | bootp | dhcp}`
Mode	Privileged EXEC

serviceport protocol dhcp

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

Default	none
Format	`serviceport protocol dhcp [client-id]`
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
```

network mac-address

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	`network mac-address` *`macaddr`*
Mode	Privileged EXEC

network mac-type

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

Default	burnedin
Format	`network mac-type {local | burnedin}`
Mode	Privileged EXEC

no network mac-type

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

Format	`no network mac-type`
Mode	Privileged EXEC

network javamode

This command specifies whether or not the switch should allow access to the Java applet in the header frame of the Web interface. When access is enabled, the Java applet can be viewed from the Web interface. When access is disabled, the user cannot view the Java applet.

Default	enabled
Format	`network javamode`
Mode	Privileged EXEC

no network javamode

This command disallows access to the Java applet in the header frame of the Web interface. When access is disabled, the user cannot view the Java applet.

Format	`no network javamode`
Mode	Privileged EXEC

show network

This command displays configuration settings associated with the switch's network interface. The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed. The network interface is always considered to be up, whether or not any member ports are up; therefore, the **`show network`** command always shows Interface Status as Up.

Note: The network interface is not supported in software version 11.0. You can use the **`show network`** command only if you already configured the network interface in software version 10.0 and then upgraded to software version 11.0. However, in that case, NETGEAR recommends that you reconfigure the management IP address with the **`ezconfig`** command.

Format	`show network`
Modes	• 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.
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	If desired, a locally administered MAC address can be configured for in-band connectivity. To take effect, 'MAC Address Type' must be set to 'Locally Administered'. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 should have the following mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique Bridge Identifier is formed which is used in the Spanning Tree Protocol.
MAC Address Type	The MAC address which should 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.
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.
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 network interface. **Note:** The network interface is not supported in software version 11.0.

Command example:

The following example displays output for the network port:

```
(admin) #show network

Interface Status.............................. Up
IP Address.................................... 10.250.3.1
Subnet Mask................................... 255.255.255.0
Default Gateway............................... 10.250.3.3
IPv6 Administrative Mode...................... Enabled
IPv6 Prefix is ............................... fe80::210:18ff:fe82:64c/64
IPv6 Prefix is ............................... 2003::1/128
IPv6 Default Router is ....................... fe80::204:76ff:fe73:423a
Burned In MAC Address......................... 00:10:18:82:06:4C
Locally Administered MAC address.............. 00:00:00:00:00:00
MAC Address Type.............................. Burned In
Configured IPv4 Protocol ..................... None
Configured IPv6 Protocol ..................... DHCP
DHCPv6 Client DUID ........................... 00:03:00:06:00:10:18:82:06:4C
IPv6 Autoconfig Mode.......................... Disabled
Management VLAN ID............................ 1
DHCP Client Identifier........................ 0NETGEAR-0010.1882.160B-vl1
```

show serviceport

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.
IPv6 Default Router	TheIPv6 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.

Term	Definition
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:

```
(admin) #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
```

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

This command gives you access to the Global Config mode. 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 Line Config mode.

Format	`configure`
Mode	Privileged EXEC

line

This command gives you access to the Line Console mode, which allows you to configure various Telnet settings and the console port, as well as to configure console login/enable authentication.

Format	`line {console | telnet | ssh}`
Mode	Global Config

Term	Definition
console	Console terminal line.
telnet	Virtual terminal for remote console access (Telnet).
ssh	Virtual terminal for secured remote console access (SSH).

Command example:

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

serial baudrate

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

Default	9600
Format	`serial baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}`
Mode	Line Config

no serial baudrate

This command sets the communication rate of the terminal interface.

Format	`no serial baudrate`
Mode	Line Config

serial timeout

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	`serial timeout` *`0-160`*
Mode	Line Config

no serial timeout

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

Format	`no serial timeout`
Mode	Line Config

set sup-console

This command allows access to the full CLI from any blade. By default, the supervisor is allowed full CLI access. You can move full CLI access among the blades, but at any time, only one blade can access the management CLI. You can issue the command on the member or backup blade. After the console is transferred to the backup blade or to a member blade, access to the full CLI on the supervisor is disabled to avoid multiple simultaneous CLI inputs. You can restore full access on the supervisor by entering the command at the supervisor serial port.

Note: Entering the command while the supervisor has full CLI access has no effect.

Note: This command is supported on M5300 and M6100 series switches only.

Format	`set sup-console`
Mode	Privileged EXEC

show serial

This command displays serial communication settings for the switch.

Format	`show serial`
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.

Term	Definition
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

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

telnet

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 {`*`ip-address`* `|` *`hostname`*`}` *`port`* `[debug] [line] [localecho]`
Modes	• Privileged EXEC • User EXEC

transport input telnet

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.

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

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

Format	`no transport input telnet`
Mode	Line Config

transport output telnet

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.

Default	enabled
Format	`transport output telnet`
Mode	Line Config

no transport output telnet

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

Format	`no transport output telnet`
Mode	Line Config

session-limit

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.

Default	5
Format	`session-limit` *number*
Mode	Line Config

no session-limit

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)

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.

Default	5
Format	`session-timeout` *minutes*
Mode	Line Config

no session-timeout

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

Format	`no session-timeout`
Mode	Line Config

telnetcon maxsessions

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` *`number`*
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

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` *`minutes`*
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

show telnet

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

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.

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.

Note: The system allows a maximum of 5 SSH sessions.

ip ssh

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

ip ssh protocol

This command is used to set or remove protocol levels (or versions) for SSH. Either SSH1 (1), SSH2 (2), or both SSH 1 and SSH 2 (1 and 2) can be set.

Default	2
Format	`ip ssh protocol [1] [2]`
Mode	Privileged EXEC

ip ssh server enable

This command enables 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.

Default	enabled
Format	`ip ssh server enable`
Mode	Privileged EXEC

no ip ssh server enable

This command disables the IP secure shell server.

Format	`no ip ssh server enable`
Mode	Privileged EXEC

sshcon maxsessions

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` *number*
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

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` *minutes*
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

show ip ssh

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.
Protocol Level	The protocol level may have the values of version 1, version 2 or both versions 1 and 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 timeout value in minutes.
Keys Present	Indicates whether the SSH RSA and DSA key files are present on the device.
Key Generation in Progress	Indicates whether RSA or DSA key files generation is currently in progress.

Management Security Commands

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

crypto certificate generate

Use this command to generate a self-signed certificate for HTTPS. The generated RSA key for SSL has a length of 1024 bits. The resulting certificate is generated with a common name equal to the lowest IP address of the device and a duration of 365 days.

Format	`crypto certificate generate`
Mode	Global Config

no crypto certificate generate

Use this command to delete the HTTPS certificate files from the device, regardless of whether they are self-signed or downloaded from an outside source.

Format	`no crypto certificate generate`
Mode	Global Config

crypto key generate rsa

Use this command to generate an RSA key pair for SSH. The new key files will overwrite any existing generated or downloaded RSA key files.

Format	`crypto key generate rsa`
Mode	Global Config

no crypto key generate rsa

Use this command to delete the RSA key files from the device.

Format	`no crypto key generate rsa`
Mode	Global Config

crypto key generate dsa

Use this command to generate a DSA key pair for SSH. The new key files will overwrite any existing generated or downloaded DSA key files.

Format	`crypto key generate dsa`
Mode	Global Config

no crypto key generate dsa

Use this command to delete the DSA key files from the device.

Format	`no crypto key generate dsa`
Mode	Global Config

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. Management ACLs are only configurable on IP (in-band) interfaces, not on the service port.

When a management ACL is enabled, incoming TCP packets initiating a connection (TCP SYN) and all UDP packets are filtered based on their source IP address and destination port. When the management ACL is disabled, incoming TCP/UDP packets are not filtered and are processed normally.

Note: Management and ACL commands are supported on M5300 and M6100 series switches only.

management access-list

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` *`name`*
Mode	Global Config

no management access-list

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

Format	`no management access list` *`name`*
Mode	Global Config

permit ip-source

This command sets permit conditions for the management access list based on the source IP address of a packet. Optionally, you can specify a subnet mask, service type, priority, or a combination of these for the rule. Each rule requires a unique priority. Use this command in Management access-list configuration mode.

Format	`permit` *`ip-source ip-address`* `[mask {`*`mask	prefix-length`*`}] [service` *`service`*`] [priority` *`priority`*`]`
Mode	Management access-list configuration

Parameter	Definition
ip-address	The source IP address.
mask	The network mask of the source IP address.
prefix-length	Specifies the number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/).
service	Indicates the service type: telnet, ssh, http, https, or snmp.
priority	The priority for the rule.

permit service

This command sets permit conditions for the management access list based on the access protocol. Each rule requires a unique priority. Use this command in Management access-list configuration mode.

Format	`permit service` *`service`* `[priority` *`priority`*`]`
Mode	Management access-list configuration

Parameter	Definition
service	Indicates the service type: telnet, ssh, http, https, or snmp.
priority	The priority for the rule.

permit priority

This command assigns a permit priority to the rule. Each rule requires a unique priority. Use this command in Management access-list configuration mode.

Format	`permit priority` *`priority`*
Mode	Management access-list configuration

deny ip-source

This command sets deny conditions for the management access list based on the source IP address of a packet. Optionally, you can specify a subnet mask, service type, priority, or a combination of these for the rule. Each rule requires a unique priority. Use this command in Management access-list configuration mode.

Format	`deny` *`ip-source ip-address`* `[mask {`*`mask`* `|` *`prefix-length`*`}] [service` *`service`*`] [priority` *`priority`*`]`
Mode	Management access-list configuration

Parameter	Definition
ip-address	The source IP address.
mask	The network mask of the source IP address.
prefix-length	Specifies the number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/).
service	Indicates the service type: telnet, ssh, http, https, or snmp.
priority	The priority for the rule.

deny service

This command sets deny conditions for the management access list based on the access protocol. Each rule requires a unique priority. Use this command in Management access-list configuration mode.

Format	`deny service` *`service`* `[priority` *`priority`*`]`
Mode	Management access-list configuration

Parameter	Definition
service	Indicates the service type: telnet, ssh, http, https, or snmp.
priority	The priority for the rule.

deny priority

This command assigns a deny priority to the rule. Each rule requires a unique priority. Use this command in Management access-list configuration mode.

Format	`deny priority` *`priority`*
Mode	Management access-list configuration

management access-class

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` *`name`*
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

This command displays information about the configured management ALC.

Format	`show management access-list [`*`name`*`]`
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 92).
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

This command displays information about the configured management ALC.

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 92).
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

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, ip https accounting exec

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

Note: The user exec accounting list should be created using the command *aaa accounting* on page 128.

Format	`ip {http | https} accounting exec {default | listname}`
Mode	Global Config

Parameter	Description
http or 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 http/https accounting exec

This command deletes the authorization method list.

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

ip http authentication

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

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

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

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 java

This command enables the Web Java mode. The Java mode applies to both secure and un-secure Web connections.

Default	Enabled
Format	`ip http java`
Mode	Privileged EXEC

no ip http java

This command disables the Web Java mode. The Java mode applies to both secure and un-secure Web connections.

Format	`no ip http java`
Mode	Privileged EXEC

ip http session hard-timeout

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` *hours*
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

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` *number*
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

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` *minutes*
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

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` *hours*
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

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` *number*
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

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` *`minutes`*
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

This command is used to set the SSL port where port can be 1025-65535 and the default is port 443.

Default	443
Format	`ip http secure-port` *`portid`*
Mode	Privileged EXEC

no ip http secure-port

This command is used to reset the SSL port to the default value.

Format	`no ip http secure-port`
Mode	Privileged EXEC

ip http secure-protocol

This command is used to set protocol levels (versions). The protocol level can be set to TLS1, SSL3 or to both TLS1 and SSL3.

Default	SSL3 and TLS1
Format	`ip http secure-protocol [SSL3] [TLS1]`
Mode	Privileged EXEC

show ip http

This command displays the http settings for the switch.

Format	`show ip http`
Mode	Privileged EXEC

Term	Definition
HTTP Mode (Unsecure)	The unsecure HTTP server administrative mode.
Java Mode	The java applet administrative mode which applies to both secure and un-secure web connections.
Maximum Allowable HTTP Sessions	The number of allowable un-secure http sessions.
HTTP Session Hard Timeout	The hard timeout for un-secure http sessions in hours.
HTTP Session Soft Timeout	The soft timeout for un-secure http sessions in minutes.
HTTP Mode (Secure)	The secure HTTP server administrative mode.
Secure Port	The secure HTTP server port number.
Secure Protocol Level(s)	The protocol level may have the values of SSL3, TSL1, or both SSL3 and TSL1.
Maximum Allowable HTTPS Sessions	The number of allowable secure http sessions.
HTTPS Session Hard Timeout	The hard timeout for secure http sessions in hours.
HTTPS Session Soft Timeout	The soft timeout for secure http sessions in minutes.
Certificate Present	Indicates whether the secure-server certificate files are present on the device.
Certificate Generation in Progress	Indicates whether certificate generation is currently in progress.

Access Commands

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

disconnect

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 loginsession`** command.

Format	`disconnect {`*`session_id`*` | all}`
Mode	Privileged EXEC

show loginsession

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

Format	`show loginsession`
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 loginsession long

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

Format	`show loginsession long`
Mode	Privileged EXEC

Command example:

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

User Account Commands

This section describes the commands you use to add, manage, and delete system users. NETGEAR Managed Switch software has two default users: admin and guest. The admin user can view and configure system settings, and the guest user can view settings.

Note: You cannot delete the admin user. There is only one user allowed with read/write privileges. You can configure up to five read-only users on the system.

aaa authentication login

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 given 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	`aaa authentication login {default | list-name} method1 [method2...]`
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	`aaa authentication login {default | list-name}`
Mode	Global Config

aaa authentication enable

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. In NETGEAR Managed Switch, 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 given 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, then NETGEAR Managed Switch does not prompt for a user name. In such cases, NETGEAR Managed Switch only prompts for a password. NETGEAR Managed 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 109 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 | list-name} method1 [method2...]`
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 | list-name}`
Mode	Global Config

aaa authorization

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	`aaa authorization {exec | commands} {default | list-name} method1 [method2…]`
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	`no aaa authorization {exec | commands} {default | <list-name>} <method1> [<method2>…]`
Mode	Global Config

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 this:

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	`aaa authorization {commands | exec} {default | list-name} method1 [method2]`
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

This command applies a command authorization method list to an access method (console, telnet, ssh). For usage scenarios on per command authorization, see the command *aaa authorization* on page 106.

Format	`authorization commands [default | list-name]`
Mode	Line console, Line telnet, Line SSH

Parameter	Description
commands	This causes command authorization for each command execution attempt.

no authorization commands

This command removes command authorization from a line config mode.

Format	`no authorization {commands | exec}`
Mode	Line console, Line telnet, Line SSH

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

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. For usage scenarios on exec authorization, see the command *aaa authorization* on page 106.

Format	`authorization exec` *`list-name`*
Mode	Line console, Line telnet, Line SSH

Parameter	Description
list-name	The command authorization method list.

no authorization exec

This command removes command authorization from a line config mode.

Format	`no authorization exec`
Mode	Line console, Line telnet, Line SSH

authorization exec default

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. For usage scenarios on exec authorization, see the command *aaa authorization* on page 106.

Format	`authorization exec default`
Mode	Line console, Line telnet, Line SSH

no authorization exec default

This command removes command authorization from a line config mode.

Format	`no authorization exec default`
Mode	Line console, Line telnet, Line SSH

show authorization methods

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

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

Format	`enable authentication {default | list-name}`
Mode	Line Config

Parameter	Description
default	Uses the default list created with the **aaa authentication enable**e command.
list-name	Uses the indicated list created with the **aaa authentication enable** 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

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

Format	`no enable authentication`
Mode	Line Config

username (Global Config)

Use the **`username`** command in Global Config mode to add a new user to the local user database. The default privilege level is 1. Using the **`encrypted`** keyword allows the administrator to transfer local user passwords between devices without having to know the passwords. When the **`password`** parameter is used along with **`encrypted`** parameter, the password must be exactly 128 hexadecimal characters in length. If the password strength feature is enabled, this command checks for password strength and returns an appropriate error if it fails to meet the password strength criteria. Giving the optional parameter **`override-complexity-check`** disables the validation of the password strength.

Format	`username` *`name`* `{password` *`password`* `[encrypted [override-complexity-check] | level` *`level`* `[encrypted [override-complexity-check]] | override-complexity-check]} | {level` *`level`* `[override-complexity-check] password}`
Mode	Global Config

Parameter	Description
name	The name of the user. Range: 1-64 characters.
password	The authentication password for the user. Range 8-64 characters. This value can be zero if the `no passwords min-length` command has been executed. The special characters allowed in the password include ! # $ % & ' ( ) * + , - . / : ; < = > @ [\ ] ^ _ ` { | } ~.
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. Enter access level 1 for Read Access or 15 for Read/Write Access. If not specified where it is optional, the privilege level is 1.
encrypted	Encrypted password entered, copied from another switch configuration.
override-complexity-check	Disables the validation of the password strength.

Command example:

The following example configures user *`bob`* with password *`xxxyyymmmm`* and user level *`15`*.

```
(NETGEAR Switch)(config)# username bob password xxxyyymmmm level 15
```

Command example:

The following example configures user *`test`* with password *`testPassword`* and assigns a user level of 1 (read-only). The password strength is not validated.

```
(NETGEAR Switch)(config)# username test password testPassword level 1
override-complexity-check
```

Command example:

```
(NETGEAR Switch) (Config)#username test password testtest
```

Command example:

```
(NETGEAR Switch) (Config)# username test password
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafbf23b528d348cdba1b
1b7ab91be842278e5e970dbfc62d16dcd13c0b864 level 1 encrypted override-complexity-check
```

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

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

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

Command example:

```
(NETGEAR Switch) (Config)# username test level 15 override-complexity-check  password

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

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

no username

Use this command to remove a user name.

Format	`no username` *name*
Mode	Global Config

username name nopassword

Use this command to remove an existing user's password (NULL password).

Format	`username` *name* `nopassword [level` *level*`]`
Mode	Global Config

Parameter	Description
name	The name of the user. Range: 1-32 characters.

Parameter	Description
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 name unlock

Use this command to allows a locked user account to be unlocked. Only a user with read/write access can reactivate a locked user account.

Format	`username` *`name`* `unlock`
Mode	Global Config

username snmpv3 accessmode

This command specifies the snmpv3 access privileges for the specified login user. The valid access mode values are **`readonly`** and **`readwrite`**. The *`username`* is the login user name for which the specified access mode applies. The default is **`readwrite`** for the admin user and **`readonly`** for all other users. You must enter the *`username`* in the same case you used when you added the user. To see the case of the user name, enter the **`show users`** command.

Defaults	• admin - readwrite • other - readonly
Format	`username snmpv3 accessmode` *`username`* `{readonly | readwrite}`
Mode	Global Config

no username snmpv3 accessmode

This command sets the snmpv3 access privileges for the specified user as **`readwrite`** for the admin user and **`readonly`** for all other users. The *`username`* value is the user name for which the specified access mode will apply.

Format	`no username snmpv3 accessmode` *`username`*
Mode	Global Config

username snmpv3 authentication

This command specifies the authentication protocol to be used for the specified user. The valid authentication protocols are **`none`**, **`md5`** or **`sha`**. If you specify **`md5`** or **`sha`**, the login password is also used as the SNMPv3 authentication password and therefore must be at least eight characters in length. The **`username`** is the user name associated with the

authentication protocol. You must enter the *username* in the same case you used when you added the user. To see the case of the user name, enter the **show users** command.

Default	no authentication
Format	username snmpv3 authentication *username* {none | md5 | sha}
Mode	Global Config

no username snmpv3 authentication

This command sets the authentication protocol to be used for the specified user to *none*. The *username* is the user name for which the specified authentication protocol is used.

Format	no username snmpv3 authentication *username*
Mode	Global Config

username snmpv3 encryption

This command specifies the encryption protocol used for the specified user. The valid encryption protocols are **des** or **none**.

If you select **des**, you can specify the required key on the command line. The encryption key must be 8 to 64 characters long. If you select the **des** protocol but do not provide a key, the user is prompted for the key. When you use the **des** protocol, the login password is also used as the snmpv3 encryption password, so it must be a minimum of eight characters. If you select **none**, you do not need to provide a key.

The *username* value is the login user name associated with the specified encryption. You must enter the *username* in the same case you used when you added the user. To see the case of the user name, enter the **show users** command.

Default	no encryption
Format	username snmpv3 encryption *username* {none | des [*key*]}
Mode	Global Config

no username snmpv3 encryption

This command sets the encryption protocol to **none**. The *username* is the login user name for which the specified encryption protocol will be used.

Format	no username snmpv3 encryption *username*
Mode	Global Config

username snmpv3 encryption encrypted

This command specifies the des encryption protocol and the required encryption key for the specified user. The encryption key must be 8 to 64 characters long.

Default	no encryption
Format	`username snmpv3 encryption encrypted` *`username`* `des` *`key`*
Mode	Global Config

show users

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

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

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]

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 [username]

Use this command to display information about the login history of users.

Format	`show users login-history [username` *name*`]`
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

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**.

Format	`login authentication {default | list-name}`
Mode	Line Configuration

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	`no login authentication {default | list-name}`
Mode	Line Configuration

password (Line Configuration)

Use the `password` command in Line Configuration mode to specify a password on a line. The default configuration is no password is specified.

Format	`password [password [encrypted]]`
Mode	Line Config

Parameter	Definition
password	Password for this level. Range: 8-64 characters
encrypted	Encrypted password to be entered, copied from another switch configuration. The encrypted password should be 128 characters long because the assumption is that this password is already encrypted with AES.

Command example:

The following example specifies a password *mcmxxyyy* on a line.

```
(NETGEAR Switch)(config-line)# password mcmxxyyy
```

Command example:

```
(NETGEAR Switch)(Config-line)# password testtest

(NETGEAR Switch) (Config-line)# password
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafbf23b528d348cdba1b
1b7ab91be842278e5e970dbfc62d16dcd13c0b864 encrypted

(NETGEAR Switch) (Config-line)# password

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

no password (Line Configuration)

Use this command to remove the password on a line.

Format	`no password`
Mode	Line Config

password (User EXEC)

This command allow 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)

Use the **`enable password`** configuration command to set a local password to control access to the privileged EXEC mode.

Format	`enable password [`*`password`*` [encrypted]]`
Mode	Privileged EXEC

Parameter	Description
password	Password string. Range: 8-64 characters.
encrypted	Encrypted password you entered, copied from another switch configuration. The encrypted password should be 128 characters long because the assumption is that this password is already encrypted with AES.

Command example:

```
(NETGEAR Switch) #enable password testtest

(NETGEAR Switch) #enable password
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafbf23b528d348cdba1b
1b7ab91be842278e5e970dbfc62d16dcd13c0b864 encrypted

(NETGEAR Switch) #enable password

Enter old password:********

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

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

no enable password (Privileged EXEC)

Use the **no enable password** command to remove the password requirement.

Format	no enable password
Mode	Privileged EXEC

passwords min-length

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 *length*
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

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	`passwords history` *`number`*
Mode	Global Config

no passwords history

Use this command to set the password history to the default value.

Format	`no passwords history`
Mode	Global Config

passwords aging

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	`passwords aging` *`days`*
Mode	Global Config

no passwords aging

Use this command to set the password aging to the default value.

Format	`no passwords aging`
Mode	Global Config

passwords lock-out

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	`passwords lock-out` *number*
Mode	Global Config

no passwords lock-out

Use this command to set the password lock-out count to the default value.

Format	`no passwords lock-out`
Mode	Global Config

passwords strength-check

Use this command to enable the password strength feature. It is used to verify the strength of a password during configuration.

Default	Disable
Format	`passwords strength-check`
Mode	Global Config

no passwords strength-check

Use this command to set the password strength checking to the default value.

Format	`no passwords strength-check`
Mode	Global Config

passwords strength maximum consecutive-characters

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` *number*
Mode	Global Config

passwords strength maximum repeated-characters

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` *number*
Mode	Global Config

passwords strength minimum uppercase-letters

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` *number*
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

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` *number*
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

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` *number*
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 minimum numeric-characters`
Mode	Global Config

passwords strength minimum special-characters

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` *number*
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 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` *number*
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

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` *keyword*
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 [`*keyword*`]`
Mode	Global Config

show passwords configuration

Use this command to display the configured password management settings.

Format	`show passwords configuration`
Mode	Privileged EXEC

Term	Definition
Minimum Password Length	Minimum number of characters required when changing passwords.
Password History	Number of passwords to store for reuse prevention.
Password Aging	Length in days that a password is valid.
Lockout Attempts	Number of failed password login attempts before lockout.
Minimum Password Uppercase Letters	Minimum number of uppercase characters required when configuring passwords.
Minimum Password Lowercase Letters	Minimum number of lowercase characters required when configuring passwords.
Minimum Password Numeric Characters	Minimum number of numeric characters required when configuring passwords.
Maximum Password Consecutive Characters	Maximum number of consecutive characters required that the password should contain when configuring passwords.
Maximum Password Repeated Characters	Maximum number of repetition of characters that the password should contain when configuring passwords.
Minimum Password Character Classes	Minimum number of character classes (uppercase, lowercase, numeric and special) required when configuring passwords.
Password Exclude-Keywords	The set of keywords to be excluded from the configured password when strength checking is enabled.

show passwords result

Use this command to display the last password set result information.

Format	`show passwords result`
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

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	aaa ias-user username *user*
Mode	Global Config

no aaa ias-user username

Use this command to remove the specified user from the internal user database.

Format	no aaa ias-user username *user*
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

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	aaa session-id [common | unique]
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

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.

Please 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 | list-name} {start-stop | stop-only |none} method1 [method2…]`
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 | list-name}`
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
```

password (AAA IAS User Config)

Use this command to specify a password for a user in the IAS database. An optional parameter **encrypted** is provided to indicate that the password given to the command is already preencrypted.

Format	`password password [encrypted]`
Mode	AAA IAS User Config

Parameter	Definition
password	Password for this level. Range: 8-64 characters
encrypted	Encrypted password to be entered, copied from another switch configuration.

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

Use this command to remove all users from the IAS database.

Format	`clear aaa ias-users`
Mode	Privileged Exec

Parameter	Definition
password	Password for this level. Range: 8-64 characters
encrypted	Encrypted password to be entered, copied from another switch configuration.

Command example:

```
(NETGEAR Switch) #
(NETGEAR Switch) #clear aaa ias-users
```

```
(NETGEAR Switch) #
```

show aaa ias-users

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) #
(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

Use this command in Line Configuration mode to apply the accounting method list to a line config (console/telnet/ssh).

Format	`accounting {exec | commands} {default | `*`list-name`*`}`
Mode	Line Configuration

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 Line Configuration mode.

Format	`no accounting {exec | commands]`
Mode	Line Configuration

show accounting

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

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
```

clear accounting statistics

This command clears the accounting statistics.

Format	`clear accounting statistics`
Mode	Privileged Exec

show domain-name

This command displays the configured domain-name.

Format	`show domain-name`
Mode	Privileged Exec

Command example:

```
(NETGEAR Switch) #
(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

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` *name* `|` `location` *loc* `|` `contact` *con*`}`
Mode	Global Config

snmp-server community

This command adds (and names) a new SNMP 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. The length of the *name* parameter can be up to 16 case-sensitive characters.

Note: 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.

Default	• Public and private, which you can rename. • Default values for the remaining four community names are blank.
Format	`snmp-server community` *name*
Mode	Global Config

no snmp-server community

This command removed a community name from the table. The *name* parameter is the community name that must be deleted.

Format	`no snmp-server community` *name*
Mode	Global Config

snmp-server community ipaddr

This command sets a client IP address for an SNMP community. 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. The name is the applicable community name.

Default	`0.0.0.0`
Format	`snmp-server community ipaddr` *`ipaddr name`*
Mode	Global Config

no snmp-server community ipaddr

This command sets a client IP address for an SNMP community to 0.0.0.0. The name is the applicable community name.

Format	`no snmp-server community ipaddr` *`name`*
Mode	Global Config

snmp-server community ipmask

This command sets a 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. The name is the applicable community name.

Default	`0.0.0.0`
Format	`snmp-server community ipmask` *`ipmask name`*
Mode	Global Config

no snmp-server community ipmask

This command sets a client IP mask for an SNMP community to 0.0.0.0. The name is the applicable community name.

Format	`no snmp-server community ipmask` *`name`*
Mode	Global Config

snmp-server community mode

This command activates an SNMP community. If a community is enabled, an SNMP manager that is associated with this community manages the switch according to its access right. If the community is disabled, no SNMP requests using this community are accepted. In

this case, the SNMP manager that is associated with this community cannot manage the switch until the status is changed back to enabled.

Default	• private and public communities - enabled • other four - disabled
Format	`snmp-server community mode` *name*
Mode	Global Config

no snmp-server community mode

This command deactivates an SNMP community. If the community is disabled, no SNMP requests using this community are accepted. In this case, the SNMP manager that is associated with this community cannot manage the switch until the status is changed back to enabled.

Format	`no snmp-server community mode` *name*
Mode	Global Config

snmp-server community ro

This command restricts access to switch information. The access mode is read-only (also called public).

Format	`snmp-server community ro` *name*
Mode	Global Config

snmp-server community rw

This command restricts access to switch information. The access mode is read/write (also called private).

Format	`snmp-server community rw` *name*
Mode	Global Config

snmp-server enable traps violation

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 Ports Commands* on page 424.

Default	disabled
Format	`snmp-server enable traps violation`
Mode	Interface Config

no snmp-server enable traps violation

This command prevents the switch from sending violation traps.

Format	`no snmp-server enable traps violation`
Mode	Interface Config

snmp-server enable traps

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 linkmode

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 142

Default	enabled
Format	`snmp-server enable traps linkmode`
Mode	Global Config

no snmp-server enable traps linkmode

This command disables Link Up/Down traps for the entire switch.

Format	`no snmp-server enable traps linkmode`
Mode	Global Config

snmp-server enable traps multiusers

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

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 bgp

The **bgp** option for the *snmp-server enable traps* command enables the two traps defined in the standard BGP MIB, RFC 4273. A trap is sent when an adjacency reaches the ESTABLISHED state and when a backward adjacency state transition occurs.

Default	BGP traps are disabled by default.
Format	`snmp-server enable traps bgp state-changes limited`
Mode	Global Config

Parameter	Description
state-changes limited	Enable standard traps defined in RFC 4273.

no snmp-server enable traps bgp

This command disables the two traps defined in the standard BGP MIB, RFC 4273.

Format	`no snmp-server enable traps bgp state-changes limited`
Mode	Global Config

snmp-server port

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	`snmp-server port` *`number`*
Mode	User 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	User EXEC

snmptrap

This command adds an SNMP trap receiver. The *`snmpversion`* parameter is the version of SNMP. The version parameter option can be **`snmpv1`** or **`snmpv2`**. You can set the SNMP trap address as an IPv4 or IPv6 global address.

The *name* parameter does not need to be unique, however; the combination of *name* and *ipaddr* or *ip6addr* must be unique. Multiple entries can exist with the same *name* as long as they are associated with a different *ipaddr* or *ip6addr*. The reverse scenario is also acceptable. The *name* is the community name used when sending the trap to the receiver, but the *name* is not directly associated with the SNMP Community table (see *snmp-server community* on page 134).

Default	snmpv2
Format	snmptrap *name* {ipaddr *ipaddr* | ip6addr *ip6addr*} [snmpversion *snmpversion*]
Mode	Global Config

Command example:

```
(NETGEAR Switch)# snmptrap mytrap ip6addr 3099::2
```

no snmptrap

This command delete trap receivers for a community.

Format	no snmptrap *name* {ipaddr *ipaddr* | ip6addr *ip6addr*}
Mode	Global Config

snmptrap snmpversion

This command modifies the SNMP version of a trap. The maximum length of the *name* parameter is 16 case-sensitive alphanumeric characters. The *snmpversion* parameter options are **snmpv1** or **snmpv2**.

Note: This command does not support a no form.

Default	snmpv2
Format	snmptrap snmpversion name {*ipaddr* | *ip6addr*} {snmpv1 | snmpv2}
Mode	Global Config

snmptrap ipaddr

This command assigns a new IP address or host name to a community name. The name can use up to 16 case-sensitive alphanumeric characters.

Note: IP addresses in the SNMP trap receiver table must be unique. If you make multiple entries using the same IP address, the first entry is retained and processed. All duplicate entries are ignored.

Format	`snmptrap ipaddr name ipaddrold ipaddrnew`
Mode	Global Config

snmptrap mode

This command activates an SNMP trap. Enabled trap receivers are active (that is, able to receive traps).

Format	`snmptrap mode name {ipaddr | ip6addr}`
Mode	Global Config

no snmptrap mode

This command deactivates an SNMP trap. Disabled trap receivers are inactive (that is, not able to receive traps).

Format	`no snmptrap mode name {ipaddr | ip6addr}`
Mode	Global Config

snmptrap source-interface

This command configures the global source interface (that is, the source IP address) for all SNMP communication between the SNMP client and the server.

Format	`snmptrap source-interface {unit/slot/port | loopback loopback-id | tunnel tunnel-id | vlan vlan-id}`
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.
tunnel-id	The tunnel interface that you want to use as the source IP address. The range of the tunnel ID is from 0 to 7.
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

This command enables link status traps for an interface.

Note: This command is valid only when the Link Up/Down Flag is enabled. For more information, see *no snmp-server enable traps bgp* on page 139.

Format	`snmp trap link-status`
Mode	Interface Config

no snmp trap link-status

This command disables link status traps for an interface.

Note: This command is valid only when the Link Up/Down Flag is enabled.

Format	`no snmp trap link-status`
Mode	Interface Config

snmp trap link-status all

This command enables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled. For more information, see *no snmp-server enable traps bgp* on page 139.

Format	`snmp trap link-status all`
Mode	Global Config

no snmp trap link-status all

This command disables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled. For more information, see *no snmp-server enable traps bgp* on page 139.

Format	`no snmp trap link-status all`
Mode	Global Config

show snmp-server

This command shows the SNMP UDP port on which the switch receives general SNMP messages.

Format	`show snmp-server`
Mode	User EXEC

Command example:

```
(NETGEAR Switch)#show snmp-server
SNMP Server Port.............................. 161
```

show snmpcommunity

This command displays SNMP community information. Six communities are supported. You can add, change, or delete communities. You do not need to reset the switch for changes to take effect.

The SNMP agent of the switch complies with SNMP Versions 1, 2, and 3. For more information about the SNMP specification, see the SNMP RFCs. The SNMP agent sends traps through TCP/IP to an external SNMP manager based on the SNMP configuration (the trap receiver and other SNMP community parameters).

Format	`show snmpcommunity`
Mode	Privileged EXEC

Term	Definition
SNMP Community Name	The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.
Client IP Address	An IP address (or portion thereof) from which this device will accept SNMP packets with the associated community. The requesting entity's IP address is ANDed with the Subnet Mask before being compared to the IP address. Note: If the Subnet Mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0.
Client IP Mask	A mask to be ANDed with the requesting entity's IP address before comparison with IP address. If the result matches with IP address then the address is an authenticated IP address. For example, if the IP address = 9.47.128.0 and the corresponding Subnet Mask = 255.255.255.0 a range of incoming IP addresses would match, i.e. the incoming IP address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0.
Access Mode	The access level for this community string.
Status	The status of this community access entry.

show snmptrap

This command displays SNMP trap receivers. Trap messages are sent across a network to an SNMP network manager. These messages alert the manager to events occurring within the switch or on the network. Six trap receivers are simultaneously supported.

Format	`show snmptrap`
Mode	Privileged EXEC

Term	Definition
SNMP Trap Name	The community string of the SNMP trap packet sent to the trap manager. The string is case-sensitive and can be up to 16 alphanumeric characters.
IP Address	The IPv4 address to receive SNMP traps from this device.
IPv6 Address	The IPv6 address to receive SNMP traps from this device.
SNMP Version	SNMPv2
Status	The receiver's status (enabled or disabled).

Command example:

```
(NETGEAR Switch)#show snmptrap

 Community Name   IpAddress     IPv6 Address     Snmp Version    Mode
 Mytrap           0.0.0.0       2001::1          SNMPv2          Enable show trapflags
```

show trapflags

This command displays the trap conditions. The command output shows all enabled trap flags, including OSPFv2 and OSPFv3 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	Can be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.
Link Up/Down Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.
Multiple Users Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether a trap will be 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).
Spanning Tree Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps are sent.
ACL Traps	May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps are sent.
BGP4 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether BGP4 traps are sent. (This field appears only on systems with the BGPv4 software package installed.)
DVMRP Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether DVMRP traps are sent.
OSPFv2 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps are sent. If any of the OSPF trap flags are not enabled, then the command displays *disabled*. Otherwise, the command shows all the enabled OSPF traps' information.
OSPFv3 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps are sent. If any of the OSPFv3 trap flags are not enabled, then the command displays *disabled*. Otherwise, the command shows all the enabled OSPFv3 traps' information.
PIM Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether PIM traps are sent.

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.

authorization network radius

Use this command to enable the switch to accept VLAN assignment by the radius server.

Default	disable
Format	`authorization network radius`
Mode	Global Config

no authorization network radius

Use this command to disable the switch to accept VLAN assignment by the radius server.

Format	`no authorization network radius`
Mode	Global Config

radius accounting mode

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

This command specifies the RADIUS client to use the NAS-IP Address attribute in the RADIUS requests. If the specific IP address is configured while enabling this attribute, the RADIUS client uses that IP address while sending NAS-IP-Address attribute in RADIUS communication.

Format	`radius server attribute 4 [`*`ipaddr`*`]`
Mode	Global Config

Term	Definition
4	NAS-IP-Address attribute to be used in RADIUS requests.
ipaddr	The IP address of the server.

no radius server attribute 4

The **no radius server attribute 4** command disables the NAS-IP-Address attribute global parameter for RADIUS client. When this parameter is disabled, the RADIUS client does not send the NAS-IP-Address attribute in RADIUS requests.

Format	no radius server attribute 4 [*ipaddr*]
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config) #radius server attribute 4  192.168.37.60
(NETGEAR Switch) (Config) #radius server attribute 4
```

radius server host

This command configures the IP address or DNS name to use for communicating with the RADIUS server of a selected server type. While configuring the IP address or DNS name for the authenticating or accounting servers, you can also configure the port number and server name. 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 and the name should be unique for accounting servers. The RADIUS client allows the configuration of a maximum 32 authenticating and accounting servers.

If you use the **auth** parameter, the command configures the IP address or host name to use to connect to a RADIUS authentication server. You can configure up to three 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. If you use the optional **port** parameter, the command configures 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, with 1813 being the default.

Note: To reconfigure a RADIUS authentication server to use the default UDP port, set the *number* argument to 1812.

If you use the **acct** token, the command configures the IP address or host name to use for the RADIUS accounting server. You can only configure one accounting server. If an accounting server is currently configured, use the **no** form of the command to remove it from the configuration. The IP address or host name you specify must match that of a previously configured accounting server. If you use the optional **port** parameter, the command

configures the UDP port to use when connecting to the RADIUS accounting server. If a port is already configured for the accounting server, the new port replaces the previously configured port. For the **port** keyword, the *number* argument must be a value in the range 0–65535, with 1813 being the default.

Note: To reconfigure a RADIUS accounting server to use the default UDP port, set the *number* argument to 1813.

Format	radius server host {auth | acct} {*ipaddr* | *dnsname*} [name *servername*] [port *number*] [type *server-type*]
Mode	Global Config

Field	Description
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
0-65535	The port number that is used to connect to the specified RADIUS server.
servername	The alias name to identify the server.
server-type	Enter one of the following options: • **0**. Specifies a standard server. • **1**. Specifies a NETGEAR server.

no radius server host

The **no radius server host** 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, then the RADIUS client selects another server for making RADIUS transactions. If the 'auth' token is used, the previously configured RADIUS authentication server is removed from the configuration. Similarly, if the 'acct' token is used, the previously configured RADIUS accounting server is removed from the configuration. The *ipaddr* 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* | *dnsname*}
Mode	Global Config

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 auth 192.168.37.60 name Network1_RS port
1813
```

```
(NETGEAR Switch) (Config) #radius server host acct 192.168.37.60 name Network2_RS
(NETGEAR Switch) (Config) #no radius server host acct 192.168.37.60
```

radius server key

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 199), 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`* `|` *`dnsname`*`} encrypted` *`password`*
Mode	Global Config

Field	Description
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
password	The password in encrypted format.

Command example:

```
radius server key acct 10.240.4.10 encrypted encrypt-string
```

radius server msgauth

This command enables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

Format	`radius server msgauth [`*`ipaddr`* `|` *`dnsname`*`]`
Mode	Global Config

Field	Description
ip addr	The IP address of the server.
dnsname	The DNS name of the server.

no radius server msgauth

The no version of this command disables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

Format	`no radius server msgauth [`*`ipaddr`* `|` *`dnsname`*`]`
Mode	Global Config

radius server primary

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	`radius server primary {`*`ipaddr`* `|` *`dnsname`*`}`
Mode	Global Config

Field	Description
ip addr	The IP address of the RADIUS Authenticating server.
dnsname	The DNS name of the server.

radius server retransmit

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	`radius server retransmit` *`retries`*
Mode	Global Config

Field	Description
retries	The maximum number of transmission attempts in the range of 1 to 15.

no radius server retransmit

The no version of this command sets the value of this global parameter to the default value.

Format	`no radius server retransmit`
Mode	Global Config

radius source-interface

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.

Format	`radius source-interface {`*`unit/slot/port`*` | loopback `*`loopback-id`*` | vlan `*`vlan-id`*`}`
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.

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 timeout

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` *`seconds`*
Mode	Global Config

Field	Description
retries	Maximum number of transmission attempts in the range 1–30.

no radius server timeout

The no version of this command sets the timeout global parameter to the default value.

Format	`no radius server timeout`
Mode	Global Config

show radius

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.
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.

Term	Definition
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

This command displays the summary and details of RADIUS authenticating servers configured for the RADIUS client.

Format	`show radius servers [`*`ipaddr`* `|` *`dnsname`* `| name [`*`servername`*`]]`
Mode	Privileged EXEC

Field	Description
ipaddr	The IP address of the authenticating server.
dnsname	The DNS name of the authenticating server.
servername	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.

Field	Description
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

Cur  Host Address              Server Name                      Port  Type
rent
---- ----------------------- -------------------------------- ----- ----------
 *   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

This command displays a summary of configured RADIUS accounting servers.

Format	`show radius accounting name [`*`servername`*`]`
Mode	Privileged EXEC

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

This command displays a summary of statistics for the configured RADIUS accounting servers.

Format	`show radius accounting statistics {`*`ipaddr`* `|` *`dnsname`* `|` `name` *`servername`*`}`
Mode	Privileged EXEC

Term	Definition
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
servername	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.

Term	Definition
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

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

This command displays the summary statistics of configured RADIUS Authenticating servers.

Format	`show radius statistics {`*`ipaddr`* `|` *`dnsname`* `| name` *`servername`*`}`
Mode	Privileged EXEC

Term	Definition
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
servername	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.

Term	Definition
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.
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.

```
(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
```

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 daemon server to encrypt all messages.

tacacs-server host

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	tacacs-server host {*ip-address* | *hostname*}
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* or *hostname* argument is the IP address or host name of the TACACS+ server.

Format	no tacacs-server host {*ip-address* | *hostname*}
Mode	Global Config

tacacs-server key

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 199), these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Format	`tacacs-server key [key-string | encrypted key-string]`
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	`no tacacs-server key key-string`
Mode	Global Config

tacacs-server keystring

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	`tacacs-server keystring`
Mode	Global Config

The following shows an example of the CLI command.

```
(NETGEAR Switch)(Config)#tacacs-server keystring
Enter tacacs key:********Re-enter tacacs key:********
```

tacacs-server source-interface

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	`tacacs-server source-interface {unit/slot/port | loopback loopback-id | vlan vlan-id}`
Mode	Global Config

Parameter	Description
unit/slot/port	The unit identifier assigned to the switch, in *`unit/slot/port`* format.

Parameter	Description
loopback-id	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.

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	`no tacacs-server source-interface`
Mode	Global Config

tacacs-server timeout

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	`tacacs-server timeout` *seconds*
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	`no tacacs-server timeout`
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 199), these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Format	key [*key-string* | encrypted *key-string*]
Mode	TACACS Config

keystring (TACACS Config)

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	keystring
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)

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.

Default	49
Format	port *port-number*
Mode	TACACS Config

priority (TACACS Config)

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.

Default	0
Format	`priority` *`priority`*
Mode	TACACS Config

timeout (TACACS Config)

Use the **`timeout`** command in TACACS Configuration mode to specify the time-out value in seconds. If no time-out value is specified, the global value is used. The *`seconds`* argument is a number in the range 1–30 seconds as specifies the time-out.

Format	`timeout` *`seconds`*
Mode	TACACS Config

show tacacs

Use the **`show tacacs`** command to display the configuration, statistics, and source interface details of the TACACS+ client.

Format	`show tacacs [`*`ip-address`*` | `*`hostname`*` | `*`client`*` | `*`server`*`]`
Mode	Privileged EXEC

Term	Definition
Host address	The IP address or hostname 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.

show tacacs source-interface

Use the **`show tacacs source-interface`** command in Global Config mode 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 199) to capture the running configuration into a script. Use the **copy** command (see *copy* on page 231) 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 (Privileged EXEC)* on page 201).

You should use scripts on systems with default configuration; however, you are not prevented from applying scripts on systems with non-default configurations.

Scripts must conform to the following rules:

- Script files are not distributed across the chassis, and remain only in the blade that is the supervisor blade 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

This command applies the commands in the script to the switch. The *scriptname* argument is the name of the script to apply.

Format	`script apply` *scriptname*
Mode	Privileged EXEC

script delete

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	`script delete {`*scriptname* `| all}`
Mode	Privileged EXEC

script list

This command lists all scripts present on the switch as well as the remaining available space.

Format	`script list`
Mode	Privileged EXEC

Term	Definition
Configuration Script	Name of the script.
Size	Privileged EXEC

script show

This command displays the contents of a script file, which you specify with the *scriptname* argument.

Format	`script show` *scriptname*
Mode	Privileged EXEC

Term	Definition
Output Format	line number: line contents

script validate

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 given script on any given device.

Format	`script validate` *scriptname*
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)

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

This command changes the name of the prompt. The length of name may be up to 64 alphanumeric characters.

Format	`set prompt` *prompt-string*
Mode	Privileged EXEC

hostname

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` *`hostname`*
Mode	Privileged EXEC

show clibanner

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

Use this command to configure the prelogin CLI banner before displaying the login prompt.

Format	`set clibanner` *`line`*
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	`no set clibanner`
Mode	Global Config

Utility Commands

7

This chapter describes the utility commands available in the NETGEAR Managed Switch CLI. 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*
- *System Utility and Clear Commands*
- *Simple 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 command**s. 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 flies 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

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

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` *number*
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

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

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

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

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

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

This command erases the stacking configuration file This configuration file cannot be erased using the clear config command.

Note: This command is supported on M5300 series switches only.

Format	`erase stack-config`
Mode	Privileged EXEC

show autoinstall

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”

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”

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”

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”

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”

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”

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”

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

NETGEAR Managed Switch software 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

This command deletes the image1 or image 2 file from the permanent storage. The optional *unit* parameter is valid only for blades. The *unit* parameter identifies the blade on which you must execute this command. When you do not enter this parameter, the command is executed on all blades in the chassis.

Format	`delete [`*unit*`] {image1 | image2}`
Mode	Privileged EXEC

boot system

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 doesn't exist on the system, this command returns an error message. The optional *unit* parameter identifies the blade on which you must execute this command. When you do not enter this parameter, the command is executed on all blades in the chassis.

Format	`boot system [`*unit*`] {image1 | image2}`
Mode	Privileged EXEC

show bootvar

This command displays the version information and the activation status for the current images on the supplied blade of the chassis. If you do not specify a blade number, the command displays image details for all nodes on the chassis. The command also displays any text description associated with an image. This command, when used on a standalone

system, displays the switch activation status. For a standalone system, the unit parameter is not valid.

Format	`show bootvar [unit]`
Mode	Privileged EXEC

filedescr

This command associates a given text description with an image. Any existing description will be replaced. The command is executed on all blades in a chassis.

Format	`filedescr {image1 | image2} text-description`
Mode	Privileged EXEC

update bootcode

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 blade on which this command must be executed. When this parameter is not supplied, the command is executed on all blades in a chassis.

Format	`update bootcode [unit]`
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)

This command displays the contents of the Address Resolution Protocol (ARP) table that is associated with the IP address of the chassis. 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.

Term	Definition
MAC Address	Hardware MAC address of that device.
Interface	For a service port the output is `Management`. For a network port, the output is the *`unit/slot/port`* of the physical interface.

show eventlog

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 [`*`unit`*`]`
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.
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

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 179.

Format	`show hardware`
Mode	Privileged EXEC

show version

This command displays inventory information for the switch.

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.
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

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

This command displays a summary of statistics for a specific interface or a count of all CPU traffic based upon the argument.

Format	`show interface {`*`unit/slot/port`* `| switchport}`
Mode	Privileged EXEC

The display parameters, when the argument is *`unit/slot/port`*, are as follows.

Parameters	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.
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 interfaces status

Use this command to display interface information, including the description, port state, speed and auto-neg capabilities. The command is similar to **show port all** but displays additional fields like interface description and port-capability.

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**. The interfaces displayed by this command are physical interfaces, LAG interfaces and VLAN routing interfaces.

Format	`show interfaces status [`*`unit/slot/port`*`]`
Mode	Privileged EXEC

Field	Description
Port	The interface associated with the rest of the data in the row.
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.

Field	Description
Flow Control Status	The 802.3x flow control status.
Flow Control	The configured 802.3x flow control mode.

show interfaces traffic

Use this command to display interface traffic information.

Format	`show interfaces traffic [`*`unit/slot/port`*`]`
Mode	Privileged EXEC

Field	Description
Interface Name	The interface associated with the rest of the data in the row.
Congestion Drops	The number of packets that have been dropped on the interface due to congestion.
TX Queue	The number of cells in the transmit queue.
RX Queue	The number of cells in the receive queue.
Color Drops: Yellow	The number of yellow (conformed) packets that were dropped.
Color Drops: Red	The number of red (exceeded) packets that were dropped.
WRED TX Queue	The number of packets in the WRED transmit queue.

show interface counters

This command reports key summary statistics for all the ports (physical/CPU/port-channel).

Format	`show interface counters`
Mode	Privileged EXEC

Term	Definition
Port	The interface associated with the rest of the data in the row.
InOctects	The total number of octets received on the interface.
InUcastPkts	The total number of unicast packets received on the interface.
InMcastPkts	The total number of multicast packets received on the interface.
InBcastPkts	The total number of broadcast packets received on the interface.
OutOctects	The total number of octets transmitted by the interface.
OutUcastPkts	The total number of unicast packets transmitted by the interface.

Term	Definition
OutMcastPkts	The total number of multicast packets transmitted by the interface.
OutBcastPkts	The total number of broadcast packets transmitted by the interface.

Command example:

```
(NETGEAR Switch) #show interface counters

Port              InOctets      InUcastPkts      InMcastPkts      InBcastPkts
--------- ---------------- ---------------- ---------------- ----------------

0/1                      0                0                0                0

Port              InOctets      InUcastPkts      InMcastPkts      InBcastPkts
--------- ---------------- ---------------- ---------------- ----------------
0/1
0/2
0/3
0/4
0/5
...
...
ch1
ch2
...
ch64
CPU                 359533                0             3044              217

Port             OutOctets     OutUcastPkts     OutMcastPkts     OutBcastPkts
--------- ---------------- ---------------- ---------------- ----------------
0/1
0/2
0/3                 131369                0                0              918
0/4
0/5
...
...
ch1
ch2
...
ch64
CPU                4025293                0            32910              120
```

show interface ethernet

This command displays detailed statistics for a specific interface or for all CPU traffic based upon the argument.

Format	`show interface ethernet {`*`unit/slot/port`* `| switchport | all}`
Mode	Privileged EXEC

When you specify a value for *`unit/slot/port`*, 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 (continued)	**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.

Term	Definition
	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. **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.

Term	Definition
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

This command displays the private VLAN mapping information for the switch interfaces.

Format	`show interface ethernet` *`interface-id`* `switchport`
Mode	Privileged EXEC

Parameter	Description
interface-id	The *`unit/slot/port`* of the switch.

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 interface lag

Use this command to display configuration information about the specified LAG interface.

Format	`show interface lag` *`lag-intf-num`*
Mode	Privileged EXEC

Parameters	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.
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 fiber-ports optics

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.

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.

Field	Description
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

                                    Output    Input
Port      Temp  Voltage  Current     Power    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 fiber-ports optics-diag

This command displays the diagnostics information of the SFP in raw data.

Format	`show fiber-ports optics-diag {all | unit/slot/port}`
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     ................
```

show fiber-ports optics-eeprom

This command displays the Electrically Erasable Programmable Read-Only Memory (EEPROM) of the SFP.

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

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 I^2C interface.

Format	`show fiber-ports optics-info {all |` *`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 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.
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

                        Link Link                                  Nominal
                      Length Length                                    Bit
                        50um 62.5um                                  Rate
Port     Vendor Name     [m] [m]  Serial Number    Part Number     [Mbps] Rev
-------- --------------- --- ---- ---------------- ---------------- ----- ----
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

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 **all** 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. 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	`show mac-addr-table [`*`macaddr vlan-id`*` | all | count | interface `*`unit/slot/port`*` | vlan `*`vlan-id`*`]`
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.
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

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	`process cpu threshold type total rising` *`threshold`* `interval` *`seconds`* `[falling` *`threshold`* `interval` *`seconds`*`]`
Mode	Global Config

Parameter	Description
rising *`threshold`*	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).
rising interval *`seconds`*	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).
falling *`threshold`*	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.
falling interval *`seconds`*	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

This command displays the user and system applications.

Format	`show process app-list`
Mode	Privileged EXEC

Parameter	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

                            Admin     Auto      Running
ID    Name            PID   Status    Restart   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 cpu

This command provides the percentage utilization of the CPU by different tasks.

Note: A busy CPU might not be caused by traffic processing but by various tasks that run simultaneously.

Format	`show process cpu`
Mode	Privileged EXEC

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

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.

Parameter	Description
VM Peak	The maximum amount of virtual memory the process has used at a given time.
FD Count	The file descriptors count for the process.

Command example:

```
(NETGEAR Switch) #show process proc-list

      Process         Application               VM Size  VM Peak
PID   Name            ID-Name              Chld  (KB)     (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

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.

This command captures the current settings of OSPFv2 and OSPFv3 trapflag status:

- If all the flags are enabled, then the command displays `trapflags all`.
- If all the flags in a particular group are enabled, then the command displays `trapflags group name all`.
- If some, but not all, of the flags in that group are enabled, the command displays `trapflags groupname flag-name`.

Format	`show running-config [all | scriptname]`
Mode	Privileged EXEC

show running-config interface

Use this command to display the running configuration for a specific interface. Valid interfaces include physical, LAG, loopback, tunnel and VLAN interfaces.

Format	`show running-config interface {unit/slot/port | lag lag-intf-num | loopback loopback-id | tunnel tunnel-id | vlan vlan-id}`
Mode	Privileged EXEC

Parameter	Description
interface	Running configuration for the specified interface.
lag-intf-num	Running configuration for the LAG interface.
loopback-id	Running configuration for the loopback interface.
tunnel-id	Running configuration for the tunnel interface.
vlan-id	Running configuration for the VLAN routing interface.

The following information is displayed for the command.

Parameter	Description
unit|slot|port	Enter an interface in unit/slot/port format.
lag	Display the running config for a specified lag interface.
loopback	Display the running config for a specified loopback interface.
tunnel	Display the running config for a specified tunnel interface.
vlan	Display the running config for a specified 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 (Privileged EXEC)

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.

Parameter	Description
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 "Quanta LB6M, 8.1.14.41, U-Boot 2009.06 (Apr 19 2011 - 15:57:06)"
!System Software Version "8.1.14.41"
!System Up Time          "0 days 0 hrs 48 mins 19 secs"
!Cut-through mode is configured as disabled
!Additional Packages     BGP-4,QOS,IPv6,IPv6 Management,Routing,Data Center
!Current SNTP Synchronized Time: Not Synchronized
!
vlan database
vlan 10
exit
configure
ipv6 router ospf
exit
line console
exit
line telnet
exit
line ssh
exit
!
--More-- or (q)uit
interface 0/1
description 'intf1'
exit
router ospf
exit
exit
```

Command example:

```
(NETGEAR Switch) #show backup-config
!Current Configuration:
!
!System Description "Quanta LB6M, 8.1.14.41, U-Boot 2009.06 (Apr 19 2011 - 15:57:06)"
!System Software Version "8.1.14.41"
!System Up Time          "0 days 0 hrs 48 mins 19 secs"
!Cut-through mode is configured as disabled
```

```
!Additional Packages     BGP-4,QOS,IPv6,IPv6 Management,Routing,Data Center
!Current SNTP Synchronized Time: Not Synchronized
!
vlan database
vlan 10
exit
configure
ipv6 router ospf
exit
line console
exit
line telnet
exit
line ssh
exit
!
--More-- or (q)uit
interface 0/1
description 'intf1'
exit
router ospf
exit
exit
```

Command example:

```
(NETGEAR Switch) #show factory-defaults
!Current Configuration:
!
!System Description "Quanta LB6M, 8.1.14.41, U-Boot 2009.06 (Apr 19 2011 - 15:57:06)"
!System Software Version "8.1.14.41"
!System Up Time          "0 days 0 hrs 48 mins 19 secs"
!Cut-through mode is configured as disabled
!Additional Packages     BGP-4,QOS,IPv6,IPv6 Management,Routing,Data Center
!Current SNTP Synchronized Time: Not Synchronized
!
vlan database
vlan 10
exit
configure
ipv6 router ospf
exit
line console
exit
line telnet
exit
line ssh
```

```
exit
!
--More-- or (q)uit
interface 0/1
description 'intf1'
exit
router ospf
exit
exit
```

dir

Use this command to list the files in flash from the CLI.

Format	dir
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.ctl
    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

This command displays switch information.

Format	`show sysinfo`
Mode	Privileged EXEC

Term	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 134.
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 134.
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 134.
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.

show tech-support

Use the **`show tech-support`** command to display system and configuration information when you contact technical support. The output of the **`show tech-support`** command combines the output of the following commands and includes log history files from previous runs:

- **`show version`**
- **`show sysinfo`**
- **`show port all`**
- **`show isdp neighbors`**
- **`show logging`**
- **`show event log`**
- **`show logging buffered`**
- **`show trap log`**
- **`show running-config`**

Enter a keyword such as **`bgp`** or **`chassis`** to display the information that is related to that feature. To display the command output on the console port, enter **`line`** keyword.

Format	`show tech-support [bgp | chassis | dot1q | dot1s | dot1s | dot3ad | isdp | layer3 | lldp | log | routing | sim | switching | system] [line]`
Mode	Privileged EXEC

length

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` *number*
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

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` *number*
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

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

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	`memory free low-watermark processor` *`threshold`*
Mode	Global Config

Parameter	Description
threshold	When CPU free memory falls below this threshold, a notification message is triggered. The range is 1–1034956 (the maximum available memory on the switch). The default is 0 (disabled).

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 temprange

Use this command to set the allowed temperature range for normal operation.

Format	`environment temprange min` *`temperature`* `max` *`temperature`*
Mode	Global Config

Parameter	Definition
min *`temperature`*	Sets the minimum allowed temperature for normal operation. The range is between –100°C and 100°C. The default is 0°C.
max *`temperature`*	Sets the maximum allowed temperature for normal operation. The range is between –100°C and 100°C. The default is 0°C.

environment trap

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.

debug environment

This command displays the error logs, including information such as zero temperature reading, number of resets, and power module failures on the switch since the last time it was rebooted.

Note: To display the debug trace, enable the *debug console* command.

Format	`debug environment`
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #debug environment
Temperature Sensors:
Slot Sensor id # of Reset
1            1             0
2            1             1
3            1             0
```

```
Power supplies:
Module Failures
------ --------
1      0
2      0
3      0
4      0
5      0
6      0
7      0
8      0
```

debug i2c

This command displays information about the health and statistics of the i2c bus. The *slot* parameter specifies the slot in which a blade is installed.

Note: To display the debug trace, enable the *debug console* command.

Format	`debug i2c` *slot*
Mode	Privileged EXEC

Logging Commands

This section describes the commands you use to configure system logging, and to view logs and the logging settings.

logging buffered

This command enables logging to an in-memory log.

Default	disabled; critical when enabled
Format	`logging buffered`
Mode	Global Config

no logging buffered

This command disables logging to in-memory log.

Format	`no logging buffered`
Mode	Global Config

logging buffered wrap

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 cli-command

This command enables the CLI command logging feature, which enables the NETGEAR Managed Switch software to log all CLI commands issued on the system.

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

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; critical when enabled
Format	`logging console [`*`severitylevel`*`]`
Mode	Global Config

no logging console

This command disables logging to the console.

Format	`no logging console`
Mode	Global Config

logging host

This command configures the logging host parameters. You can configure up to eight hosts.

Default	• port—514 • level—critical (2)
Format	`logging host <hostaddress | hostname> addresstype [port-number [<severitylevel>]]`
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.
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

This command enables logging host reconfiguration.

Format	`logging host reconfigure hostindex`
Mode	Global Config

Parameter	Description
hostindex	Enter the Logging Host Index for which to change the IP address.

logging host remove

This command disables logging to host. See *show logging hosts* on page 215 for a list of host indexes.

Format	`logging host remove` *`hostindex`*
Mode	Global Config

logging port

This command sets the local port number of the LOG client for logging messages. The *`portid`* argument is a number in the range from 1 to 65535.

Default	514
Format	`logging port` *`portid`*
Mode	Global Config

no logging port

This command resets the local logging port to the default.

Format	`no logging port`
Mode	Global Config

logging syslog

This command enables syslog logging.

Format	`logging syslog`
Mode	Global Config

no logging syslog

This command disables syslog logging.

Format	`no logging syslog`
Mode	Global Config

logging syslog port

This command enables syslog logging. The *portid* argument is an integer in the range 1–65535.

Default	disabled
Format	`logging syslog port` *portid*
Mode	Global Config

no logging syslog port

This command disables syslog logging.

Format	`no logging syslog port`
Mode	Global Config

logging syslog source-interface

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.

Note: The **`serviceport`** keyword is supported only on the M6100 series switches.

Format	`logging syslog source-interface {`*unit/slot/port* `| {loopback` *loopback-id*`} | {vlan` *vlan-id*`} {tunnel` *tunnel-id* `| serviceport}}`
Mode	Global Config

Parameter	Description
unit/slot/port	VLAN or port-based routing interface.
loopback-id	Configures the loopback interface to use as the source IP address. The range of the loopback ID is 0 to 7.
tunnel-id	Configures the tunnel interface to use as the source IP address. The range of the tunnel 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.

Command example:

```
(config)#logging syslog source-interface loopback 0
(config)#logging syslog source-interface tunnel 0
(config)#logging syslog source-interface 0/4/1
(config)#logging syslog source-interface 1/0/1
```

no logging syslog source-interface

This command disables syslog logging.

Format	`no logging syslog`
Mode	Global Config

show logging

This command displays logging configuration information.

Format	`show logging`
Mode	Privileged EXEC

Term	Definition
Logging Client Local Port	Port on the collector/relay to which syslog messages are sent.
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 to log to the console log. Messages with an equal or lower numerical severity are logged.
Buffered Logging	Shows whether buffered logging is enabled.
Persistent Logging	Shows whether persistent logging is enabled.
Persistent Logging Severity Filter	The minimum severity at which the logging entries are retained after a system reboot.
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 Source Interface     : (not configured)
CLI Command Logging                 : disabled
Console Logging                     : enabled
Console Logging Severity Filter     : error
Buffered Logging                    : enabled
Persistent Logging                  : disabled
Persistent Logging Severity Filter  : alert

Syslog Logging                      : disabled

Log Messages Received               : 1010
Log Messages Dropped                : 0
Log Messages Relayed                : 0
```

show logging buffered

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.

show logging hosts

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).
Port	The server port number, which is the port on the local host from which syslog messages are sent.
Host Status	The state of logging to configured syslog hosts. If the status is disable, no logging occurs.

Command example:

```
(NETGEAR Switch) #show logging hosts

Index  IP Address/Hostname         Severity   Port     Status
-------- --------------------- -----------  ------  --------
1         10.130.64.88             critical     514    Active
2         2000::150                critical     514    Active
```

show logging persistent

Use the **show logging persistent** command to display persistent log entries.

Format	show logging persistent
Mode	Privileged EXEC

Parameter	Description
Persistent Log Count	The number of persistent log entries.

Command example:

```
(NETGEAR switch) #show logging persistent

Persistent Logging: disabled
Persistent Log Count: 0
```

show logging traplogs

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

This command clears buffered logging (system startup and system operation logs).

Format	`clear logging buffered`
Mode	Privileged EXEC

clear eventlog

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

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 [`*`severitylevel`*`]`
Mode	Global Config

no logging email

This command disables email alerting.

Format	`no logging email`
Mode	Global Config

logging email urgent

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 {`*`severitylevel`*` | 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

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` *`to-email-addr`*
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` *`to-email-addr`*
Mode	Global Config

logging email from-addr

This command configures the email address of the sender (the switch).

Default	switch@netgear.com
Format	`logging email from-addr` *`from-email-addr`*
Mode	Global Config

no logging email from-addr

This command removes the configured email source address.

Format	`no logging email from-addr` *`from-email-addr`*
Mode	Global Config

logging email message-type subject

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` *`subject`*
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

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` *`minutes`*
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

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` *`severitylevel`*
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

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` *`message-body`*
Mode	Global Config

show logging email config

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).

Term	Definition
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.
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

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

This command resets the email alerting statistics.

Format	`clear logging email statistics`
Mode	Privileged EXEC

mail-server

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	`mail-server {`*`ip-address`* `|` *`ipv6-address`* `|` *`hostname`*`}`
Mode	Global Config

no mail-server

This command removes the specified SMTP server from the configuration.

Format	`no mail-server {`*`ip-address`* `|` *`ipv6-address`* `|` *`hostname`*`}`
Mode	Global Config

security

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	`security {tlsv1 | none}`
Mode	Mail Server Config

port (Mail Server Config)

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	`port` *`number`*
Mode	Mail Server Config

username (Mail Server Config)

This command configures the login ID the switch uses to authenticate with the SMTP server.

Default	admin
Format	`username` *`name`*
Mode	Mail Server Config

password (Mail Server Config)

This command configures the password the switch uses to authenticate with the SMTP server.

Default	admin
Format	`password` *`password`*
Mode	Mail Server Config

show mail-server config

This command displays information about the email alert configuration.

Format	`show mail-server {`*`ip-address`* `|` *`hostname`* `| all} 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.

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

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.

A NETGEAR Managed Switch does not accept an incoming packet, such as a traceroute response, 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). Similarly, NETGEAR Managed Switch will 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.

Default	count: 3 probes interval: 3 seconds size: 0 bytes port: 33434 maxTtl: 30 hops maxFail: 5 probes initTtl: 1 hop
Format	`traceroute {`*`ip-address`* `|` `[ipv6] {`*`ipv6-address`* `|` *`hostname`*`}} [initTtl` *`initTtl`*`] [maxTtl` *`maxTtl`*`] [maxFail` *`maxFail`*`] [interval` *`interval`*`] [count` *`count`*`] [port` *`port`*`] [size` *`size`*`] [source {`*`ip-address`* `|` *`ipv6-address`* `|` *`unit/slot/port`*`}]`
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 *`ipaddress`* value should be a valid IP address.
ipv6-address	The *`ipv6-address`* value should be a valid IPv6 address.
hostname	The *`hostname`* value should be a valid hostname.
ipv6	The optional **`ipv6`** keyword can be used before *`ipv6-address`* or *`hostname`*. Giving the **`ipv6`** keyword before the *`hostname`* tries it to resolve to an IPv6 address.

Parameter	Description
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 **maxTtle** 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

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.

Format	`clear config`
Mode	Privileged EXEC

clear counters

This command clears the statistics for a specified *unit/slot/port,* for all the ports, or for the entire switch based upon the argument.

Format	`clear counters {`*`unit/slot/port`*` | all}`
Mode	Privileged EXEC

clear mac-addr-table

This command clears the dynamically learned MAC addresses of the switch.

Format	`clear mac-addr-table`
Mode	Privileged EXEC

clear igmpsnooping

This command clears the tables managed by the IGMP Snooping function and attempts to delete these entries from the Multicast Forwarding Database.

Format	`clear igmpsnooping`
Mode	Privileged EXEC

clear pass

This command resets all user passwords to the factory defaults without powering off the switch. You are prompted to confirm that the password reset should proceed.

Format	`clear pass`
Mode	Privileged EXEC

clear traplog

This command clears the trap log.

Format	`clear traplog`
Mode	Privileged EXEC

clear vlan

This command resets VLAN configuration parameters to the factory defaults. When the VLAN configuration is reset to the factory defaults, there are some scenarios regarding GVRP and MVRP that happen due to this:

1. Static VLANs are deleted.
2. GVRP is restored to the factory default as a result of handling the VLAN RESTORE NOTIFY event. Since GVRP is disabled by default, this means that GVRP should be disabled and all of its dynamic VLANs should be deleted.
3. MVRP is restored to the factory default as a result of handling the VLAN RESTORE NOTIFY event. Since MVRP is enabled by default, this means that any VLANs already created by MVRP are unaffected. However, for customer platforms where MVRP is disabled by default, then the MVRP behavior should match GVRP. That is, MVRP is disabled and the MVRP VLANs are deleted.

Format	`clear vlan`
Mode	Privileged EXEC

logout

This command closes the current telnet connection or resets the current serial connection.

Note: Save configuration changes before logging out.

Format	`logout`
Modes	Privileged EXEC User EXEC

ping

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.

Note: For information about the `ping` command for IPv6 hosts, see *ping ipv6* on page 927.

Default	The default count is 1. The default interval is 3 seconds. The default size is 0 bytes.
Format	`ping {`*`address`*`| `*`hostname`*` | {ipv6 {interface {`*`unit/slot/port`*` | vlan `*`vlan-id`*` | loopback `*`loopback-id`*` | network | serviceport | tunnel `*`tunnel-id`*` } `*`link-local-address`*`} | `*`ipv6-address`*` | `*`hostname`*`} [count `*`count`*`] [interval `*`seconds`*`] [size `*`size`*`] [source `*`ip-address`*` | `*`ipv6-address`*` | {`*`unit/slot/port`*` | vlan `*`vlan-id`*` | serviceport | network}]`
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
address	IPv4 or IPv6 addresses to ping.
count	Use the **count** parameter to specify the number of ping packets (ICMP Echo requests) that are sent to the destination address specified by the *ip-address* field. The range for *count* is 1 to 15 requests.
interval	Use the **interval** parameter to specify the time between Echo Requests, in seconds. Range is 1 to 60 seconds.
size	Use the **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 **source** parameter to specify the source IP/IPv6 address or interface to use when sending the Echo requests packets.
hostname	Use the **hostname** parameter to resolve to an IPv4 or IPv6 address. The **ipv6** keyword is specified to resolve the host name to IPv6 address. The IPv4 address is resolved if no keyword is specified.
ipv6	The optional keyword **ipv6** can be used before the *ipv6-address* or *hostname* argument. Using the **ipv6** optional keyword before *hostname* tries to resolve it directly to the IPv6 address. Also used for pinging a link-local IPv6 address.
interface	Use the *interface* keyword to ping a link-local IPv6 address over an interface.
link-local-address	The link-local IPv6 address to ping over an interface.

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
```

quit

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)

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

copy

The **copy** command uploads and downloads files to and from the switch. You can also use the **copy** command to 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	copy *source destination* {verify | noverify}
Mode	Privileged EXEC

Replace the *source* and *destination* parameters with the options in *Table 9* on page 232. For the *url* source or destination, use one of the following values:

```
copy {<url> | image1 | image2 | nvram:backup-config | nvram:clibanner |
nvram:cpu-pkt-capture.pcap | nvram:errorlog | nvram:factory-defaults | nvram:log |
nvram:script | nvram:startup-config | nvram:tech-support | nvram:traplog |
system:running-config} {<url> | isa-users | image1 | image2 | nvram:startup-config |
nvram:backup-config | nvram:startup-config | nvram:clibanner | nvram:script
<destfilename> | nvram:script <destfilename> noval | nvram:sshkey-dsa |
nvram:sshkey-rsa1 | nvram:sshkey-rsa2 | nvram:sslpem-dhweak | nvram:sslpem-dhstrong |
nvram:sslpem-root | nvram:sslpem-server:nvram:startup-config} {verify | noverify}
```

verify and **noverify** are only available if the image/configuration verify options feature is enabled (see *file verify* on page 235); **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: *ip6address* is also a valid parameter for routing packages that support IPv6.

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}`
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.

Table 9. Copy parameters

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:operational-log`	`url`	Copies the operational log file to a server.
`nvram:script` *scriptname*	*url*	Copies a specified configuration script file to a server.
`nvram:startup-config`	`nvram:backup-config`	Copies the startup configuration to the backup configuration.
`nvram:startup-config`	*url*	Copies the startup configuration to a server.
`nvram:startup-log`	`url`	Uploads the startup log file.

Table 9. Copy parameters (continued)

Source	Destination	Description
`nvram:traplog`	*`url`*	Copies the trap log file to a server.
`system:running-config`	`nvram:startup-config`	Saves the running configuration to NVRAM.
`system:running-config`	`nvram:factory-defaults`	Saves the running configuration to NVRAM to the `factory-defaults` file.
`system:image`	`url`	Saves the system image to a server.
`url`	`nvram:clibanner`	Downloads the CLI banner to the system.
`url`	`nvram:publickey-config`	Downloads the Public Key for Configuration Script validation.
`url`	`nvram:publickey-image`	Downloads Public Key for Image validation.
`url`	`nvram:script` *`destfilename`*	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.
`url`	`nvram:script` *`destfilename`* `noval`	When you use this option, the copy command will 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`		
`url`	`nvram:sshkey-dsa`	Downloads an SSH key file. For more information, see *Secure Shell Commands* on page 86.
`url`	`nvram:sshkey-rsa1`	Downloads an SSH key file.
`url`	`nvram:sshkey-rsa2`	Downloads an SSH key file.
`url`	`nvram:sslpem-dhweak`	Downloads an HTTP secure-server certificate.
`url`	`nvram:sslpem-dhstrong`	Downloads an HTTP secure-server certificate.
`url`	`nvram:sslpem-root`	Downloads an HTTP secure-server certificate. For more information, see *Hypertext Transfer Protocol Commands* on page 94.
`url`	`nvram:sslpem-server`	Downloads an HTTP secure-server certificate.
`url`	`nvram:startup-config`	Downloads the startup configuration file to the system.
`url`	`ias-users`	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.

Table 9. Copy parameters (continued)

Source	Destination	Description
url	{image1 | image2}	Download an image from the remote server to either image. The downloaded image is distributed to the chassis blades.
{image1 | image2}	*url*	Upload either image to the remote server.
url	nvram:tech-support-cmds	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-suport dot3ad** command and the **show tech-support ospf** command.
{image1 | image2}	unit://*unit*/{image1 | image2}	Copy an image from the management blade to a given blade in a chassis. Use the unit parameter to specify the blade to which the image should be copied.
{image1 | image2}	unit://*/{image1 | image2}	Copy an image from the management blade to all blades in a chassis.

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

This command enables digital signature verification while an image and/or configuration file is downloaded to the switch.

Note: This command is supported on M6100 series switches only.

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.
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

write memory

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	`write memory [confirm]`
Mode	Privileged EXEC

Simple Network Time Protocol Commands

This section describes the commands you use to automatically configure the system time and date by using Simple Network Time Protocol (SNTP).

sntp broadcast client poll-interval

This command sets the poll interval for SNTP broadcast clients in seconds as a power of two where *poll-interval* can be a value from 6 to 10.

Default	6
Format	sntp broadcast client poll-interval *poll-interval*
Mode	Global Config

no sntp broadcast client poll-interval

This command resets the poll interval for SNTP broadcast client back to the default value.

Format	no sntp broadcast client poll-interval
Mode	Global Config

sntp client mode

This command enables Simple Network Time Protocol (SNTP) client mode and may set the mode to either broadcast or unicast.

Default	disabled
Format	sntp client mode [broadcast | unicast]
Mode	Global Config

no sntp client mode

This command disables Simple Network Time Protocol (SNTP) client mode.

Format	no sntp client mode
Mode	Global Config

sntp client port

This command sets the SNTP client port ID to a value in the range 1025–65535, represented by the *portid* argument. The default value is 0, which means that the SNTP port is not configured by the user. In the default case, the actual client port value used in SNTP packets is assigned by the underlying OS.

Default	0
Format	sntp client port *portid*
Mode	Global Config

no sntp client port

This command resets the SNTP client port back to its default value.

Format	`no sntp client port`
Mode	Global Config

sntp unicast client poll-interval

This command sets the poll interval for SNTP unicast clients in seconds as a power of two where *`poll-interval`* can be a value from 6 to 10.

Default	6
Format	`sntp unicast client poll-interval` *`poll-interval`*
Mode	Global Config

no sntp unicast client poll-interval

This command resets the poll interval for SNTP unicast clients to its default value.

Format	`no sntp unicast client poll-interval`
Mode	Global Config

sntp unicast client poll-timeout

This command sets the poll time-out for SNTP unicast clients to a value from 1–30 seconds, as represented by the *`poll-timeout`* argument.

Default	5
Format	`sntp unicast client poll-timeout` *`poll-timeout`*
Mode	Global Config

no sntp unicast client poll-timeout

This command will reset the poll timeout for SNTP unicast clients to its default value.

Format	`no sntp unicast client poll-timeout`
Mode	Global Config

sntp unicast client poll-retry

This command sets the poll retry for SNTP unicast clients to a value from 0 to 10, as represented by the *`poll-retry`* argument.

Default	1
Format	`sntp unicast client poll-retry` *`poll-retry`*
Mode	Global Config

no sntp unicast client poll-retry

This command will reset the poll retry for SNTP unicast clients to its default value.

Format	`no sntp unicast client poll-retry`
Mode	Global Config

sntp server

This command configures an SNTP server (a maximum of three). The server address can be either an IPv4 address or an IPv6 address. The optional *`priority`* can be a value of 1–3, the *`version`* a value of 1–4, and the *`portid`* a value of 1–65535.

Format	`sntp server {`*`ipaddress`* `|` *`ipv6address`* `|` *`hostname`*`} [`*`priority`* `[`*`version`* `[`*`portid`*`]]]`
Mode	Global Config

no sntp server

This command deletes an server from the configured SNTP servers.

Format	`no sntp server remove {`*`ipaddress`* `|` *`ipv6address`* `|` *`hostname`*`}`
Mode	Global Config

sntp source-interface

Use this command to specify the physical or logical interface to use as the source interface (source IP address) for SNTP unicast server configuration. If configured, the address of source Interface is used for all SNTP communications between the SNTP server and the SNTP 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 SNTP client falls back to its default behavior.

Format	`sntp source-interface {`*`unit/slot/port`* `|` `loopback` *`loopback-id`* `|` `vlan` *`vlan-id`*`}`
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.
tunnel-id	Configures the IPv6 tunnel interface. The range of the tunnel 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.

no sntp source-interface

Use this command to reset the SNTP source interface to the default settings.

Format	`no sntp source-interface`
Mode	Global Config

show sntp

This command is used to display SNTP settings and status.

Format	`show sntp`
Mode	Privileged EXEC

Term	Definition
Last Update Time	Time of last clock update.
Last Attempt Time	Time of last transmit query (in unicast mode).
Last Attempt Status	Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).
Broadcast Count	Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.

show sntp client

This command is used to display SNTP client settings.

Format	`show sntp client`
Mode	Privileged EXEC

Term	Definition
Client Supported Modes	Supported SNTP Modes (Broadcast or Unicast).
SNTP Version	The highest SNTP version the client supports.

Term	Definition
Port	SNTP Client Port. The field displays the value 0 if it is default value. When the client port value is 0, if the client is in broadcast mode, it binds to port 123; if the client is in unicast mode, it binds to the port assigned by the underlying OS.
Client Mode	Configured SNTP Client Mode.

show sntp server

This command is used to display SNTP server settings and configured servers.

Format	`show sntp server`
Mode	Privileged EXEC

Term	Definition
Server Host Address	IP address or hostname of configured SNTP Server.
Server Type	Address type of server (IPv4, IPv6, or DNS).
Server Stratum	Claimed stratum of the server for the last received valid packet.
Server Reference ID	Reference clock identifier of the server for the last received valid packet.
Server Mode	SNTP Server mode.
Server Maximum Entries	Total number of SNTP Servers allowed.
Server Current Entries	Total number of SNTP configured.

For each configured server.

Term	Definition
IP Address / Hostname	IP address or hostname of configured SNTP Server.
Address Type	Address Type of configured SNTP server (IPv4, IPv6, or DNS).
Priority	IP priority type of the configured server.
Version	SNTP Version number of the server. The protocol version used to query the server in unicast mode.
Port	Server Port Number.
Last Attempt Time	Last server attempt time for the specified server.
Last Update Status	Last server attempt status for the server.
Total Unicast Requests	Number of requests to the server.
Failed Unicast Requests	Number of failed requests from server.

show sntp source-interface

Use this command to display the SNTP client source interface configured on the switch.

Format	`show sntp source-interface`
Mode	Privileged EXEC

Field	Description
SNTP Client Source Interface	The interface ID of the physical or logical interface configured as the SNTP client source interface.
SNTP Client Source IPv4 Address	The IP address of the interface configured as the SNTP client source interface.

Command example:

```
(NETGEAR Switch) #show sntp source-interface

SNTP Client Source Interface.................. (not configured)
```

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

This command sets the system time and date.

Format	`clock set` *`hh:mm:ss`* `clock set` *`mm/dd/yyyy`*
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

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	`clock summer-time date {`*`date month`* `year` *`hh:mm date month`* `year` *`hh:mm`*`}[offset` *`offset`*`] [zone` *`acronym`*`]`
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.
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

This command sets the summer-time recurring parameters.

Format	`clock summer-time recurring {`*`week day month hh:mm week day month hh:mm`*`}` `[offset` *`offset`*`] [zone` *`acronym`*`]`
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.

Parameter	Description
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

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

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

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

This command configures a DHCP address pool name on a DHCP server and enters DHCP pool configuration mode.

Default	none
Format	`ip dhcp pool` *name*
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` *`name`*
Mode	Global Config

client-identifier

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` *`uniqueidentifier`*
Mode	DHCP Pool Config

no client-identifier

This command deletes the client identifier.

Format	`no client-identifier`
Mode	DHCP Pool Config

client-name

This command specifies the name for a DHCP client. Name is a string consisting of standard ASCII characters.

Default	none
Format	`client-name` *`name`*
Mode	DHCP Pool Config

no client-name

This command removes the client name.

Format	`no client-name`
Mode	DHCP Pool Config

default-router

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` *address1* [*address2....address8*]
Mode	DHCP Pool Config

no default-router

This command removes the default router list.

Format	`no default-router`
Mode	DHCP Pool Config

dns-server

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` *address1* [*address2....address8*]
Mode	DHCP Pool Config

no dns-server

This command removes the DNS Server list.

Format	`no dns-server`
Mode	DHCP Pool Config

hardware-address

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` *hardwareaddress type*
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

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` *`address`* `[`*`mask`* `|` *`prefix-length`*`]`
Mode	DHCP Pool Config

no host

This command removes the IP address of the DHCP client.

Format	`no host`
Mode	DHCP Pool Config

lease

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 [{`*`days`* `[`*`hours`*`] [`*`minutes`*`] | 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)

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` *`networknumber`* `[`*`mask`* `|` *`prefixlength`*`]`
Mode	DHCP Pool Config

no network

This command removes the subnet number and mask.

Format	`no network`
Mode	DHCP Pool Config

bootfile

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

This command deletes the boot image name.

Format	`no bootfile`
Mode	DHCP Pool Config

domain-name

This command specifies the domain name for a DHCP client. The *`domain`* specifies the domain name string of the client.

Default	none
Format	`domain-name` *`domain`*
Mode	DHCP Pool Config

no domain-name

This command removes the domain name.

Format	`no domain-name`
Mode	DHCP Pool Config

domain-name enable

This command enables the domain name functionality in NETGEAR Managed Switch.

Format	`domain-name enable [name` *`name`*`]`
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config)#domain-name enable
(NETGEAR Switch) (Config)#exit
```

no domain-name enable

This command disables the domain name functionality in NETGEAR Managed Switch.

Format	`no domain-name enable`
Mode	Global Config

netbios-name-server

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

The command configures the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients.type 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` *`type`*
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

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` *`address`*
Mode	DHCP Pool Config

no next-server

This command removes the boot server list.

Format	`no next-server`
Mode	DHCP Pool Config

option

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	option *code* {*ascii string* | *hex string1* [*string2...string8*] | ip *address1* [*address2...address8*]}
Mode	DHCP Pool Config

no option

This command removes the DHCP Server options. The *code* parameter specifies the DHCP option code.

Format	no option *code*
Mode	DHCP Pool Config

ip dhcp excluded-address

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 *lowaddress* [*highaddress*]
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 *lowaddress* [*highaddress*]
Mode	Global Config

ip dhcp ping packets

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` *`number`*
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

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

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

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

clear ip dhcp binding

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. *`address`* is a valid IP address made up of four decimal bytes ranging from 0 to 255. IP address **`0.0.0.0`** is invalid.

Format	`clear ip dhcp binding {`*`address`*` | *}`
Mode	Privileged EXEC

clear ip dhcp server statistics

This command clears DHCP server statistics counters.

Format	`clear ip dhcp server statistics`
Mode	Privileged EXEC

clear ip dhcp conflict

The command is used to clear an address conflict from the DHCP Server database. The server detects conflicts using a ping. DHCP server clears all conflicts If ***** (the asterisk character) is used as the address parameter.

Default	none
Format	`clear ip dhcp conflict {`*`address`*` | *}`
Mode	Privileged EXEC

show ip dhcp binding

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 [`*`address`*`]`
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

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

This command displays pool configuration. If **all** is specified, configuration for all the pools is displayed.

Format	`show ip dhcp pool configuration {`*name* `| all}`
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.
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

This command displays DHCP server statistics.

Format	`show ip dhcp server statistics`
Modes	Privileged EXEC User EXEC

Field	Definition
Automatic Bindings	The number of IP addresses that have been automatically 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.

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 conflict

This command displays address conflicts logged by the DHCP Server. If no IP address is specified, all the conflicting addresses are displayed.

Format	`show ip dhcp conflict [`*`ip-address`*`]`
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 hostname lookup service to other components of NETGEAR Managed Switch.

ip domain lookup

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

Use this command to define a default domain name that NETGEAR Managed Switch software 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` *name*
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

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` *`name`*
Mode	Global Config

no ip domain list

Use this command to delete a name from a list.

Format	`no ip domain list` *`name`*
Mode	Global Config

ip name server

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`*s is a valid IPv4 or IPv6 address of the server. The preference of the servers is determined by the order they were entered.

Format	`ip name-server` *`server-address1`* [*`server-address2...server-address8`*]
Mode	Global Config

no ip name server

Use this command to remove a name server.

Format	`no ip name-server [`*`server-address1...server-address8`*`]`
Mode	Global Config

ip name source-interface

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.

Format	`ip name source-interface {`*`unit/slot/port`* `| loopback` *`loopback-id`* `| tunnel` *`tunnel-id`* `| vlan` *`vlan-id`*`}`
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

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` *`name ipaddress`*
Mode	Global Config

no ip host

Use this command to remove the name-to-address mapping.

Format	`no ip host` *`name`*
Mode	Global Config

ipv6 host

Use this command to define static host name-to-IPv6 address mapping in the host cache. The parameter *name* is host name and *v6 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` *`name v6 address`*
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` *`name`*
Mode	Global Config

ip domain retry

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` *`number`*
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

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` *`seconds`*
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

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 {`*`name`*` | all}`
Mode	Privileged EXEC

Field	Description
name	A particular host entry to remove. The parameter *name* ranges from 1-255 characters.
all	Removes all entries.

show hosts

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 *name* ranges from 1-255 characters. This command displays both IPv4 and IPv6 entries.

Format	`show hosts [`*`name`*`]`
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.

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 Switching> 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

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

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

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 of network engineers to diagnose conditions affecting their NETGEAR Managed Switch product.



CAUTION:

The output of debug commands can be long and may adversely affect system performance.

capture start

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

Use the **`capture stop`** command to manually stop capturing CPU packets for packet trace.

Format	`capture stop`
Mode	Privileged EXEC

capture {file | remote | line}

Use this command to configure file capture options. The command is persistent across a reboot cycle.

Format	`capture {file | remote | line}`
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**.

Parameter	Description
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.

capture remote port

Use this command to configure file capture options. The command is persistent across a reboot cycle. The *id* argument is a TCP port number from 1024– 49151.

Format	`capture remote port` *id*
Mode	Global Config

capture file size

Use this command to configure file capture options. The command is persistent across a reboot cycle. The *max-file-size* argument is the maximum size the pcap file can reach, which is 2–512 KB.

Format	`capture file size` *max file size*
Mode	Global Config

capture line wrap

This command enables wrapping of captured packets in line mode when the captured packets reaches full capacity.

Format	`capture line wrap`
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	`no capture line wrap`
Mode	Global Config

show capture packets

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	`show capture packets`
Mode	Privileged EXEC

debug aaa accounting

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	`debug aaa accounting`
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

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 arp

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

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.

Default	none
Format	`debug authentication packet {all | event} interface` *`unit/slot/port`*
Mode	Privileged EXEC

debug auto-voip

Use this command to enable Auto VoIP debug messages. Use the optional parameters to trace H323, SCCP, SIP, OUI packets respectively.

Note: To display the debug trace, enable the *debug console* command.

Default	disabled
Format	`debug auto-voip [H323 | SCCP |SIP | oui]`
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 clear

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

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.

Note: To display the debug trace, enable the *debug console* command.

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

Use this command 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 chassis 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)
- /proc 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 | deteteall | [kernel] crashlog-number [upload url]| data crashlog-number [download url | upload url | component-id item-number additional-parameter]} [slot slot]`
Mode	Privileged EXEC

Parameter	Description
kernel	View the crash log file for the kernel
crashlog-number	Specifies the file number to view. The system maintains up to four copies, and the valid range is 1–4.
upload *url*	To upload the crash log (or crash dump) to a TFTP server, use the **upload** keyword and specify the required TFTP server information.
proc	View the application process crashlog.
verbose	Enable the verbose crashlog.
deleteall	Delete all crash log files on the system.
data	Crash log data recorder.
crashdump-number	Specifies the crash dump number to view. The valid range is 0–2.
download *url*	To download a crash dump to the switch, use the **download** 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.
slot	The slot number for the blade on which the crashlog is located.

debug dcbx packet

Use this command to enable debug tracing for DCBX packets that are transmitted or received.

Note: To display the debug trace, enable the *debug console* command.

Default	disabled
Format	`debug dcbx packet {receive | transmit}`
Mode	Privileged EXEC

debug debug-config

Use this command to download or upload the debug-config.ini file. The debug-config. ini file executes CLI commands (including devshell and drivshell 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	`debug debug-config {download` *`url`* `| upload` *`url`*`}`
Mode	Privileged EXEC

debug dhcp packet

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	`debug dhcp packet [transmit | receive]`
Mode	Privileged EXEC

no debug dhcp

This command disables the display of “debug” trace output for DHCPv4 client activity.

Format	`no debug dhcp packet [transmit | receive]`
Mode	Privileged EXEC

debug dot1x packet

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`
Mode	Privileged EXEC

no debug dot1x packet

Use this command to disable dot1x packet debug trace.

Format	`no debug dot1x`
Mode	Privileged EXEC

debug fip-snooping packet

Use this command in Privileged EXEC mode to enable FIP packet debug trace on transmit or receive path with different filter options configured.

Note: To display the debug trace, enable the *debug console* command.

Default	disabled
Format	`debug fip-snooping packet [{transmit | receive | filter {dst-mac` *`mac-addr`* `| fip-proto-code` *`code`* `| src-intf` *`unit/slot/port`* `| src-mac` *`mac-addr`* `| vlan vlan-`*`id`*`}]`
Mode	User EXEC Privileged EXEC

Parameter	Description
dst-mac	If the dst-mac filter option is given, trace output is filtered on matching the given Destination MAC Address.
fip-proto-code	If the fip-proto-code filter option is given, trace output is filtered on matching the supported types. The *code* variable can be in the range 1–15.
src-intf	If the src-intf filter option is given, trace output is filtered on matching the incoming source interface.
src-mac	If the src-mac filter option is given, trace output is filtered on matching the given Source MAC Address.
vlan *vlan-id*	If the vlan filter option is given, trace output is filtered on matching the given VLAN ID. The *id* variable can be in the range 1–4093.

no debug fip-snooping packet

Use this command in Privileged EXEC mode to disable FIP packet debug trace on transmit or receive path with different filter options configured.

Format	`no debug fip-snooping packet [{transmit | receive | filter {dst-mac` *`mac-addr`* `| fip-proto-code` *`code`* `| src-intf` *`unit/slot/port`* `| src-mac` *`mac-addr`* `| vlan` *`vlan-id`*`}]`
Mode	User EXEC Privileged EXEC

debug igmpsnooping packet

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`
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

This command enables tracing of IGMP Snooping packets transmitted by the switch. Snooping should 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

A sample output of the trace message is shown below.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[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/slot/port (internal interface number). Unit is always shown as 1 for interfaces on a standalone device.
Src_Mac	Source MAC address of the packet.
Dest_Mac	Destination multicast MAC address of the packet.

Parameter	Definition
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

This command enables tracing of IGMP Snooping packets received by the switch. Snooping should 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

A sample output of the trace message is shown below.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[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.

Parameter	Definition
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

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` *`number`*
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 bgp (serviceability packet tracing)

Use this command to enable BGP packet debug trace. Debug messages are sent to the system log at the DEBUG severity level. To print the debug messages to the console, enable console logging at the DEBUG level using the command **`logging console debug`**. The debug options enabled for a specific peer are the union of the options enabled globally and the options enabled specifically for the peer. Enabling one of the packet type options enables packet tracing in both the inbound and outbound directions.

Note: To display the debug trace, enable the *debug console* command.

Default	disabled
Format	`debug ip bgp {`*`ipv4-address`* `|` *`ipv6-address`*`} [events | in | interface {`*`unit/slot/port`* `|` `vlan` *`vlan-id`*`} | keepalives | notification | open | out | refresh | updates]`
Mode	Privileged EXEC

Parameter	Description
peer-address	(Optional) The IPv4 address of a BGP peer. Debug traces are enabled for a specific peer when this option is specified. The command can be issued multiple times to enable simultaneous tracing for multiple peers.
events	(Optional) Trace adjacency state events.
keepalives	(Optional) Trace transmit and receive of KEEPALIVE packets.
notification	(Optional) Trace transmit and receive of NOTIFICATION packets.
open	(Optional) Trace transmit and receive of OPEN packets.
refresh	(Optional) Traces transmit and receive of ROUTE REFRESH packets.
updates	(Optional) Traces transmit and receive of UPDATE packets.

no debug bgp

Use this command to disable debug tracing of BGP events.

Format	`no debug ip bgp [`*`peer-address`* `| events | keepalives | notification | open | refresh | updates]`
Mode	Privileged EXEC

debug ip dvmrp packet

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

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

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

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

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 ip vrrp

Use this command to enable VRRP debug protocol messages.

Note: To display the debug trace, enable the *debug console* command.

Default	disabled
Format	`debug ip vrrp`
Mode	Privileged EXEC

no debug ip vrrp

Use this command to disable VRRP debug protocol messages.

Format	`no debug ip vrrp`
Mode	Privileged EXEC

debug ipv6 dhcp

This command displays “debug” information about DHCPv6 client activities and traces DHCPv6 packets to and from the local DHCPv6 client.

Note: To display the debug trace, enable the *debug console* command.

Default	disabled
Format	`debug ipv6 dhcp`
Mode	Privileged EXEC

no debug ipv6 dhcp

This command disables the display of “debug” trace output for DHCPv6 client activity.

Format	`no debug ipv6 dhcp`
Mode	Privileged EXEC

debug ipv6 mcache packet

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

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 ospfv3 packet

Use this command to enable IPv6 OSPFv3 packet debug trace.

Note: To display the debug trace, enable the *debug console* command.

Default	disabled
Format	`debug ipv6 ospfv3 packet`
Mode	Privileged EXEC

no debug ipv6 ospfv3 packet

Use this command to disable tracing of IPv6 OSPFv3 packets.

Format	`no debug ipv6 ospfv3 packet`
Mode	Privileged EXEC

debug ipv6 pimsm packet

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. When neither keyword is used in the command, then 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

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

A sample output of the trace message is shown below.

```
<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 mldsnooping packet

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 ospf packet

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

Sample outputs of the trace messages are shown below.

```
<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
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.

Parameter	Definition
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 ping packet

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

A sample output of the trace message is shown below.

```
<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 rip packet

This command turns on tracing of RIP requests and responses. This command takes no options. 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

A sample output of the trace message is shown below.

```
<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.

Parameter	Definition
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

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

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

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

A sample output of the trace message is shown below.

```
<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

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

A sample output of the trace message is shown below.

```
<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

Use the **debug tacacs packe**t command to turn on TACACS+ debugging.

Note: To display the debug trace, enable the *debug console* command.

Format	debug tacacs {packet [receive | transmit] | accounting | authentication}
Mode	Global Config

Parameter	Description
packet receive	Turn on TACACS+ receive packet debugs.
packet transmit	Turn on TACACS+ transmit packet debugs.
accounting	Turn on TACACS+ authentication debugging.
authentication	Turn on TACACS+ authorization debugging.

debug transfer

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 udld events

This command enables debugging for the UDLD events.

Note: To display the debug trace, enable the *debug console* command.

Default	Disabled
Format	debug udld events
Mode	Privileged EXEC

debug udld packet receive

This command enables debugging on the received UDLD PDUs.

Note: To display the debug trace, enable the *debug console* command.

Default	`Disabled`
Format	`debug udld packet receive`
Mode	Privileged EXEC

debug udld packet transmit

This command enables debugging on the transmitted UDLD PDUs.

Note: To display the debug trace, enable the *debug console* command.

Default	`Disabled`
Format	`debug udld packet transmit`
Mode	Privileged EXEC

show debugging

Use the **`show debugging`** 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 the **`no show debugging`** command to disable packet tracing configurations.

Format	`no show debugging`
Mode	Privileged EXEC

exception protocol

Note: The NFS, TFTP, and FTP protocols are supported on the M6100 series switches only.

Use this command to specify the protocol used to store the core dump file.

Default	usb
Format	`exception protocol {nfs | tftp | ftp| usb | none}`
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

Note: The FTP protocol is supported on the M6100 series switches only.

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` *`ip-address`* `[{username` *`user-name`* `password` *`password`*`}]`
Mode	Global Config

no exception dump ftp-server

Note: The FTP protocol is supported on the M6100 series switches only.

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

Note: The TFTP protocol is supported on the M6100 series switches only.

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 {`*`ip-address`*`}`
Mode	Global Config

no exception dump tftp-server

Note: The TFTP protocol is supported on the M6100 series switches only.

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 nfs

Note: The NFS protocol is supported on the M6100 series switches only.

Use this command to configure an NFS mount point in order to dump core file to the NFS file system.

Default	None
Format	`exception dump nfs` *`ip-address/dir`*
Mode	Global Config

no exception dump nfs

Note: The NFS protocol is supported on the M6100 series switches only.

Use this command to reset the exception dump NFS mount point configuration to its factory default value.

Format	`no exception dump nfs`
Mode	Global Config

exception dump filepath

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` *`dir`*
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

Use this command to enable compression mode.

Note: This command is supported on M6100 series switches only

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

This command configures the protocol (DHCP or static) that is used to configure the service port after a unit crashed. If you specify **dhcp**, the unit receives its IP address from a DHCP server that must be available in the network.

Note: This command is supported on M6100 series switches only

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

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.

Note: This command is supported on M6100 series switches only

Default	None
Format	exception dump stack-ip-address add *ip-address netmask* [*gateway*]
Mode	Global Config

exception dump stack-ip-address remove

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.

Note: This command is supported on M6100 series switches only

Format	no exception dump stack-ip-address remove *ip-address netmask*
Mode	Global Config

exception core-file

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	exception core-file {*file-name-prefix* | [hostname] | [time-stamp]}
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	no exception core-file
Mode	Global Config

exception switch-chip-register

Use this command to enable or disable the switch-chip-register dump in case of an exception. The switch-chip-register dump occurs only for the supervisor unit and not for member units.

Default	Disable
Format	exception switch-chip-register {enable | disable}
Mode	Global Config

exception nmi

This command enables or disables a core dump for an nonmaskable interrupt (NMI).

Default	Disable
Format	exception nmi {enable | disable}
Mode	Global Config

write core

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 **write core test**, 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 [*dest_file_name*]]
Mode	Privileged EXEC

show exception

Use this command to display the configuration parameters for generating a core dump file.

Default	None
Format	show exception
Mode	Privileged EXEC

Command example:

```
Protocol exception protocol configuration
TFTP Server Address            TFTP server configuration
NFS Mount point                NFS mount point configuration
Core File name prefix          Core file prefix configuration.
Hostname                       Core file name contains hostname if enabled.
Timestamp                      Core file name contains timestamp if enabled.
Switch Chip Register Dump      Switch chip register dump configuration
```

logging persistent

Use this command to configure the Persistent logging for the switch. The severity level of logging messages is specified at severity level. Possible values for severity level are **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), or **debug** (7).

Default	Disable
Format	logging persistent *severitylevel*
Mode	Global Config

no logging persistent

Use this command to disable the persistent logging in the switch.

Format	`no logging persistent`
Mode	Global Config

mbuf

Use this command to configure memory buffer (MBUF) threshold limits and generate notifications when MBUF limits have been reached.

Format	`mbuf {falling-threshold | rising threshold | severity}`
Mode	Global Config

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 at which Mbuf logs messages. The range is 1 to 7. The default is 5 (L7_LOG_SEVERITY_NOTICE).

show mbuf

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

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.

show msg-queue

Use this command to display the message queues.

Default	None
Format	`show msg-queue`
Mode	Privileged Exec

session start unit

Use this command to initiate a console session from the supervisor blade to a member blade in the chassis. During the session, troubleshooting and debugging commands can be issued on the supervisor blade, and the output displays the relevant information from the member blade specified in the session.

Default	Disable
Format	`session start unit` *`unit-number`*
Mode	Privileged Exec

sw reset

Use this command to reboot the switch after a serious error occurred.

Default	Enabled
Format	`sw reset`
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	`no sw reset`
Mode	Global Config

show sw reset

Use this command to show whether the **`sw reset`** command is enabled.

Format	`show sw reset`
Mode	User EXEC

Support Mode Commands

Support mode is hidden and available when the **techsupport enable** command is executed. The tech support mode is disabled by default. Configurations related to support mode are shown in the **show tech-support** command. They can be persisted by using the command **save** in support mode. Support configurations are stored in a separate binary config file, which cannot be uploaded or downloaded.

techsupport enable

Use this command to allow access to Support mode.

Default	Disabled
Format	`techsupport enable`
Mode	Privileged Exec

console

Use this command to enable the display of support debug for this session.

Default	Disabled
Format	`console`
Mode	Support

save

Use this command to save the trace configuration to non-volatile storage.

Format	`save`
Mode	Support

snapshot bgp

Use the snapshot bgp command in Support mode to dump a set of BGP debug information to capture the current state of BGP.

Note: This command is supported on M6100 series switches only

Format	`snapshot bgp`
Mode	Support mode

snapshot ospf

Use this command in Support mode to dump a set of OSPF debug information to capture the current state of OSPF. The output is written to the console and can be extensive.

Note: This command is supported on M6100 series switches only

Format	`snapshot ospf`
Mode	Support mode

snapshot routing

Use this command in Support mode to dump a set of routing debug information to capture the current state of routing on the switch. The output is written to the console and can be extensive.

Format	`snapshot routing`
Mode	Support

snapshot multicast

Use this command in Support mode to dump a set of IP multicast debug information to capture the current state of multicast on the switch. The output is written to the console and can be extensive.

Note: This command is supported on M5300 and M6100 series switches only

Format	`snapshot multicast`
Mode	Support

snapshot system

Use this command in Support mode to dump a set of system debug information to capture the current state of the device. The output is written to the console and can be extensive.

Format	`snapshot multicast`
Mode	Support

telnetd

Use this command in Support mode to start or stop the Telnet daemon on the switch.

Format	`telnetd {start | stop}`
Mode	Support

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 cable. It is not supported for optical fiber cable.

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

This command returns the status of the specified port.

Format	`cablestatus` *`unit/slot/port`*
Mode	Privileged EXEC

Field	Description
Cable Status	One of the following statuses is returned: • `Normal`. The cable is working correctly. • `Open`. The cable is disconnected or there is a faulty connector. • `Short`. There is an electrical short in the cable. • `Cable Test Failed`. 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 Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded. Unknown is displayed if the cable length could not be determined.

Power Management Commands

Note: Power management commands are supported on the M6100 series switches only.

power auto-rebalance

This command enables chassis automatically re-adjusts power allocation to the blades such that lowest priority port on the chassis gets automatically shut down and higher priority ports on the chassis are powered.

Default	disabled
Format	`power auto-rebalance`
Mode	Chassis Global Config

no power auto-rebalance

This command disables auto power rebalance among blades in the chassis.

Format	`no power auto-rebalance`
Mode	Chassis Global Config

power redundancy

This command enables the N+1 power redundancy feature. If this feature is enabled and the PSU that provides 12 V power to the chassis fails, one other PSU can seamlessly take over the general supply of 12 V power to the entire chassis and all blades.

Default	Disabled
Format	`power redundancy`
Mode	Chassis 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	Chassis Global Config

power system

This command configures the total chassis system power (12V power) for the base blades.

Default	110W per blade
Format	`power system 12v_power`
Mode	Chassis Global Config

Note: The switch compares the value that you enter with the total required system power. If the value that you enter is too low, the switch generates the following message before executing the command:
`Warning: setting system power system power may cause blade or PoE ports to shut down. Are you sure you want to continue? (y/n):`
If you enter **y**, the system power is updated as requested; Otherwise, the system power is not updated.

no power system

This command reset the total chassis system power to the default value of 600.

Format	`no power system`
Mode	Chassis Global Config

show power redundancy

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 matrix

This command displays the Blade Power Matrix (BPM) table information from the hardware.

Format	`show power matrix`
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch)#show power matrix
Blade Type        Blade Model       Power Required
0x1               XCM8944            65W
0x2               XCM8944F          110W
0x3               XCM8948            50W
0x4               XCM8924X          185W
```

show power

This command displays the chassis power usage.

Format	`show power`
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch)#show power
Chassis power:
Total available power(W): ..................... 910
Total required system power(W): ............... 220
Total consumption power(W): ................... 2550
System Power(W): .............................. 220
Power auto-rebalance: ......................... Disable
Power Module AC Input: ........................ 220V
Power module redundancy (N+1): ................ Disable

                        Current      Blade
      Blade             power        power
Slot  Type   Blade Model  consumption  Required   Blade status
----  -----  -----------  -----------  ---------  ----------------
2     3      XCM8948      50 W         50 W       OK
3     2      XCM8944F     330 W        110 W      OK
```

power cycle

This command power cycles the blade, waits a few seconds, and then powers on the blade again.

Format	`power cycle` *slot*
Mode	Privileged EXEC

power rebalance

This command powers down a low priority PD device until enough power is obtained to power up a new blade.

Format	`power rebalance`
Mode	Privileged EXEC

If all PD devices are shut down but power is still not available, the switch generates the following error message on the console and in the logging buffer:

```
Insufficient power, Blade on Slot <slot number> not powered up
```

USB commands

If a USB flash device is installed in the USB slot, the USB commands display the device status and content.

show usb device

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

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
F1.cfg    256      4/22/2009 8:00:12

Total Size: xxxx
Bytes Used: yyyy
Bytes Free: zzzz
```

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

Use this command to configure the sFlow collector parameters (owner string, receiver time-out, max datagram size, IP address, and port).

Format	`sflow receiver` *`rcvr_idx`* `{owner` *`owner-string`* `{timeout` *`rcvr_timeout`* `| notimeout} | maxdatagram` *`size`* `| ip` *`ip`* `| port` *`port`*`}`
Mode	Global Config

Parameter	Description
Receiver Owner	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.
Receiver Timeout	The time, in seconds, remaining before the sampler or poller is released and stops sending samples to receiver. A management entity wanting to maintain control of the sampler is responsible for setting a new value before the old one expires. The allowed range is 0-2147483647 seconds. The default is zero (0).
No Timeout	The configured entry will be in the config until you explicitly removes the entry.
Receiver Max Datagram Size	The maximum number of data bytes that can be sent in a single sample datagram. The management entity should set this value to avoid fragmentation of the sFlow datagrams. The allowed range is 200 to 9116). The default is 1400.
Receiver IP	The sFlow receiver IP address. If set to 0.0.0.0, no sFlow datagrams will be 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` *`rcvr_idx`* `[owner | maxdatagram | ip | port]`
Mode	Global Config

sflow receiver owner timeout

Use this command to configure a receiver as a timeout entry. As the sFlow receiver is configured as a timeout entry, information related to sampler and pollers are also shown in the running-config and are retained after 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` *`index`* `owner` *`owner-string`* `timeout`
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.

sflow receiver owner notimeout

Use this command to configure a receiver as a non-timeout entry. Unlike entries configured with a specific timeout value, this command will be shown in show running-config and retained after reboot. As the sFlow receiver is configured as a non-timeout entry, information related to sampler and pollers will also be shown in the running-config and will be retained after 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` *`index`* `owner` *`owner-string`* `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.

sflow sampler

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 *rcvr_indx* is valid.

Format	`sflow sampler {`*`rcvr-indx`*` | 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.
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: `threshold value = 2^24/ (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: `configured sampling rate is 60000` `threshold value = 2^24/ (60000) = 279 (from integer division)` `recalculated sampling rate = 2^24/ (279) = 60133`

no sflow sampler

Use this command to reset the sFlow sampler instance to the default settings.

Format	`no sflow sampler {`*`rcvr-indx`* `| rate` *`sampling-rate`* `| maxheadersize` *`size`*`}`
Mode	Interface Config

sflow poller

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 *`rcvr_indx`* is valid.

Format	`sflow poller {`*`rcvr-indx`* `| interval` *`poll-interval`*`}`
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

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.

Format	`sflow source-interface {`*`unit/slot/port`* `| loopback` *`loopback-id`* `| tunnel` *`tunnel-id`* `| vlan` *`vlan-id`*`}`
Mode	Global Config

Parameter	Description
unit/slot/port	VLAN or port-based routing interface.
loopback-id	Configures the loopback interface to use as the source IP address. The range of the loopback ID is 0 to 7.
tunnel-id	Configures the tunnel interface to use as the source IP address. The range of the tunnel 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.

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

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

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 (slot/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

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 Owner                            Timeout    Max Dgram Port  IP Address
Indx String                                      Size
---- -------------------------------- ---------- --------- ----- ---------------
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

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 (slot/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

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

A Switch Database Management (SDM) template is a description of the maximum resources a switch or router can use for various features. Different SDM templates allow different combinations of scaling factors, enabling different allocations of resources depending on how the device is used. In other words, SDM templates enable you to reallocate system resources to support a different mix of features based on your network requirements.

Note: If you insert a blade in a chassis and its template does not match the template of the chassis, the blade reboots automatically using the template that is used by other chassis members. To avoid the automatic reboot, first set the template to the template that is used by existing members of the chassis. Then power off the new blade, insert it in the chassis, and power on the blade.

Note: These commands are supported on M5300 and M6100 series switches only.

sdm prefer

Use this command to change the template that will be active after the next reboot. The keywords are as follows:

- **`dual-ipv4-and-ipv6 data-center`**. Filters subsequent template choices to those that support both IPv4 and IPv6. The template maximizes the number of IPv4 and IPv6 unicast routes, while limiting the number of ECMP next hops in each route to 16.
- **`ipv4-routing data-center plus`**. Filters subsequent template choices to those that support IPv4, and not IPv6. The IPv4-only template maximizes the number of IPv4 unicast routes, while limiting the number of ECMP next hops in each route to 16.

Note: After setting the template, you must reboot in order for the configuration change to take effect.

Default	dual IPv4 and IPv6 template
Format	`sdm prefer {dual-ipv4-and-ipv6 data-center | ipv4-routing data-center plus}`
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

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.

Use the optional keywords to list the scaling parameters of a specific template.

Format	`show sdm prefer [dual-ipv4-and-ipv6 data-center | ipv4-routing data-center plus]`
Mode	Privileged EXEC

Syntax	Description
dual-ipv4-and-ipv6 data-center	(Optional) List the scaling parameters for the Dual IPv4 and IPv6 template supporting more ECMP next hops.
ipv4-routing data-center plus	(Optional) List the scaling parameters for the IPv4-only template maximizing the number of unicast routes and also supporting more ECMP next hops.

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 user has not changed the next active SDM template:

```
(NETGEAR Switch)#show sdm prefer

The current template is the Dual IPv4 and IPv6 template.

ARP Entries..................................... 6144
IPv4 Unicast Routes............................. 8160
IPv6 NDP Entries................................ 2560
IPv6 Unicast Routes............................. 4096
ECMP Next Hops.................................. 4
IPv4 Multicast Routes........................... 1536
IPv6 Multicast Routes........................... 512
```

Command example:

The following example shows the SDM template when the user sets the next active SDM template:

```
(NETGEAR Switch) # configure

(NETGEAR Switch) (Config)#sdm prefer ipv4-routing data-center default

Changes to the running SDM preferences have been stored, but cannot take effect until the
next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.

(NETGEAR Switch) (Config)#ex

(NETGEAR Switch) #show sdm prefer

The current template is the Dual IPv4 and IPv6 template.

ARP Entries..................................... 6144
IPv4 Unicast Routes............................. 8160
IPv6 NDP Entries................................ 2560
IPv6 Unicast Routes............................. 4096
ECMP Next Hops.................................. 4
IPv4 Multicast Routes........................... 1536
IPv6 Multicast Routes........................... 512

On the next reload, the template will be the IPv4 Data Center template.
```

Command example:

The following example lists the scaling parameters for the data center template:

```
(NETGEAR Switch) #show sdm prefer ipv4-routing data-center default

ARP Entries..................................... 6144
IPv4 Unicast Routes............................. 8160
IPv6 NDP Entries................................ 0
IPv6 Unicast Routes............................. 0
ECMP Next Hops.................................. 16
IPv4 Multicast Routes........................... 2048
IPv6 Multicast Routes........................... 0
```

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. NETGEAR Managed Switch software supports the following three Green Ethernet modes:

- Energy-detect mode
- Energy-efficient Ethernet (EEE) mode

Note: Green Ethernet commands are supported on M6100 and M7100 series switches only.

green-mode energy-detect

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.

Note: .This command is supported on M6100 series switches only.

Default	disabled
Format	`green-mode energy-detect`
Mode	Interface Config

no green-mode energy-detect

Use this command to disable energy-detect mode on the interface(s).

Format	`no green-mode energy-detect`
Mode	Interface Config

green-mode eee

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	`green-mode eee`
Mode	Interface Config

no green-mode eee

Use this command to disable EEE mode on the interface(s).

Format	`no green-mode eee`
Mode	Interface Config

green-mode eee tx-idle-time

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.

Note: This command is supported on M6100 series switches only.

Default	0
Format	`green-mode eee tx-idle-time` *`microseconds`*
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

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.

Note: This command is supported on M6100 series switches only.

Default	0
Format	`green-mode eee tx-wake-time` *microseconds*
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

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).

Note: 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` *seconds*
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

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` *size*
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

Use this command to display the green-mode configuration and operational status on all ports or on the specified port.

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 Chassis	Estimated cumulative energy saved in the chassis in (watts * hours) due to all green modes enabled
Current Power Consumption per Chassis	Power consumption by all ports in the chassis in mWatts.
Power Saving	Estimated percentage power saved on all ports in the chassis due to Green mode(s) enabled.

Term	Definition
Unit	Unit Index of the chassis member.
Green Ethernet Features supported	List of Green Features supported on the given 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) #show green-mode

Current Power Consumption (mW)..............  11172
Power Saving (%)............................  10
Cumulative Energy Saving /Chassis (W * H)...  10

Unit  Green Ethernet Features Supported
----  -------------------------------
1     Energy-Detect EEE LPI-History LLDP-Cap-Exchg Pwr-Usg-Est

Interface     Energy-Detect      Short-Reach-Config    Short-Reach    EEE
            Config       Opr     Auto        Forced       Opr        Config
---------  ---------  ---------  ---------  ---------  -----------   --------
1/0/1      Enabled    Active     Enabled    Disabled   Inactive      Enabled
1/0/2      Enabled    Active     Enabled    Disabled   Inactive      Enabled
1/0/3      Enabled    Active     Enabled    Disabled   Inactive      Enabled
1/0/4      Enabled    Active     Enabled    Disabled   Inactive      Enabled
1/0/5      Enabled    Active     Enabled    Disabled   Inactive      Enabled
1/0/6      Enabled    Active     Enabled    Disabled   Inactive      Enabled
1/0/7      Enabled    Active     Enabled    Disabled   Inactive      Enabled
--More-- or (q)uit
```

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 *No energy detected.*
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.
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.

Term	Definition
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
```

clear green-mode statistics

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.

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 325) retain their data.

Format	`clear green-mode statistics {`*`unit/slot/port`* `| all}`
Mode	Privileged EXEC

show green-mode eee-lpi-history

Use this command to display interface green-mode EEE LPI history.

Format	`green-mode eee-lpi-history interface` *`unit/slot/port`*
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 chassis	Percentage of Total time spent in LPI mode by all port in a chassis 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 Chassis.................. 29

                            Percentage of    Percentage of
Sample     Time Since       Time spent in   Time spent in
 No.       The Sample       LPI mode since   LPI mode since
          Was Recorded      last sample      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
```

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

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

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 (*`alarm-number`*)	An arbitrary integer index value used to uniquely identify the high capacity alarm entry. The range is 1 to 65535.
High Capacity Alarm Variable (*`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 (*`sample-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`** 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.

Parameter	Description
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 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 monitorHCAlarm.
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` *`alarm-number`*
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config)# no rmon hcalarm 1
```

rmon event

This command sets the RMON event entry in the RMON event MIB group.

Format	`rmon event` *`event-number`* `[description` *`string`* `| log | owner` *`string`* `| trap` *`community`*`]`
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	`no rmon event` *`event-number`*
Mode	Global Config

Command example:

```
(NETGEAR Switch) (Config)# no rmon event 1
```

rmon collection history

This command sets the history control parameters of the RMON historyControl MIB group.

Note: This command is not supported on 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` *`index-number`* `[buckets` *`number`* `| interval` *`seconds`* `| owner` *`string`*`]`
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

This command displays the entries in the RMON alarm table.

Format	`show rmon {alarms | alarm` *`alarm-index`*`}`
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

This command displays the entries in the RMON history control table.

Format	`show rmon collection history [interfaces` *`unit/slot/port`*`]`
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.

Command example:

```
(NETGEAR Switch) #show rmon collection history

Index   Interface    Interval   Requested   Granted     Owner
                                 Samples     Samples
-------------------------------------------------------------------
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   Granted     Owner
                                 Samples     Samples
-------------------------------------------------------------------
1       1/0/1        30         10          10          myowner
2       1/0/1        1800       50          10          monitorHistoryControl
```

show rmon events

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

This command displays the specified entry in the RMON history table.

Format	`show rmon history` *`index`* `{errors [period` *`seconds`*`] | other [period` *`seconds`*`] | throughput [period` *`seconds`*`]}`
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.
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


(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
Jan 01 1970 21:46:15 0          0         0         0          1


(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
Jan 01 1970 21:42:14 0       0
Jan 01 1970 21:42:44 0       0
Jan 01 1970 21:43:14 0       0
Jan 01 1970 21:43:44 0       0
Jan 01 1970 21:44:14 0       0
Jan 01 1970 21:44:45 0       0
Jan 01 1970 21:45:15 0       0
Jan 01 1970 21:45:45 0       0
Jan 01 1970 21:46:15 0       0
```

show rmon log

This command displays the entries in the RMON log table.

Format	`show rmon log [`*`event-index`*`]`
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

This command displays the RMON statistics for the given interfaces.

Format	`show rmon statistics interfaces` *`unit/slot/port`*
Mode	Privileged Exec

Term	Description
Port	unit/slot/port
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.
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).

Term	Description
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

This command displays the entries in the RMON high-capacity alarm table.

Format	`show rmon hcalarms [`*`alarm-index`*`]`
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.
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.

Term	Description
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 thie 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 monitorHCAlarm.
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.

Note: This command is supported on M6100 series switches only.

stats group (Global Config)

This command creates a new group with the specified id or name and configures the time range and the reporting mechanism for that group.

Format	`stats group` *`group-id`* `|` *`name`* `timerange` *`time-range name`* `reporting` *`list-of-reporting-methods`*
Mode	Global 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.
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.
list of reporting methods	Report the statistics to the configured method. The range is: • **0**. none • **1**. console • **2**. syslog • **3**. e-mail The default is None.

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 [`*`group-id`* `|` *`name`*`]`
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)

This command configures flow based statistics rules for the given parameters over the specified time range. Only an IPv4 address is allowed as source and destination IP address

Format	`stats flow-based` *`rule-id`* `timerange` *`time-range-name`* `[{srcip` *`ip-address`*`} {dstip` *`ip-address`*`} {srcmac` *`mac-address`*`} {dstmac` *`mac-address`*`} {srctcpport` *`portid`*`} {dsttcpport` *`portid`*`} {srcudpport` *`portid`*`} {dstudpport` *`portid`*`}]`
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.
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 srctcpport 123 dsttcpport 123 srcudpport 123 dstudpport  123


(NETGEAR Switch) (Config)#stats flow-based 2 timerange test srcip 1.1.1.1 dstip 2.2.2.2
srctcpport 123 dsttcpport 123 srcudpport 123 dstudpport 123
```

no stats flow-based

This command deletes flow-based statistics.

Format	`stats flow-based` *`rule-id`*
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

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.

Format	`stats flow-based reporting` *`list-of-reporting-methods`*
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)

This command applies the group specified on an interface or interface-range.

Format	`stats group [`*`group-id`* `|` *`name`*`]`
Mode	Interface Config

Parameter	Description
group id	The unique identifier for the group.
name	The name of the group.

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 group specified.

Format	`no stats group [`*`group-id`* `|` *`name`*`]`
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)

This command applies the flow-based rule specified by the ID on an interface or interface-range.

Format	`stats flow-based` *`rule-id`*
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	`no stats flow-based` *`rule-id`*
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

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	`show stats group [`*`group-id`* `|` *`name`*`]`
Mode	Privileged EXEC

Parameter	Description
group id	The unique identifier for the group.
name	The name of the group.

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

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
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
```

Switching Commands

8

This chapter describes the switching commands available in the NETGEAR Managed Switch CLI.

The Switching Commands chapter includes the following sections:

- *Port Configuration Commands*
- *Spanning Tree Protocol Commands*
- *VLAN Commands*
- *Switch Port Commands*
- *Double VLAN Commands*
- *Private VLAN Commands*
- *Voice VLAN Commands*
- *Provisioning (IEEE 802.1p) Commands*
- *Asymmetric Flow Control*
- *Protected Ports Commands*
- *Private Group Commands*
- *GARP Commands*
- *GVRP Commands*
- *GMRP Commands*
- *Port-Based Network Access Control Commands*
- *802.1X Supplicant Commands*
- *Storm-Control Commands*
- *Link Local Protocol Filtering Commands*
- *MRP Commands*
- *MMRP Commands*
- *MVRP Commands*
- *MVRP Commands*
- *Port-Channel/LAG (802.3ad) Commands*
- *Port Mirroring Commands*
- *Static MAC Filtering Commands*

- *DHCP L2 Relay Agent Commands*
- *DHCP Client Commands*
- *DHCP Snooping Configuration Commands*
- *Dynamic ARP Inspection 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*
- *UniDirectional Link Detection Commands*
- *Link Debounce 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)

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	`interface {`*`unit/slot/port	unit/slot/port-unit/slot/port`*`}`
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

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

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)

Use this command to create an alpha-numeric description of an interface or range of interfaces.

Format	`description` *`description`*
Mode	Interface Config

mtu

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. For the standard NETGEAR Managed Switch implementation, the MTU size is a valid integer between 1522–9216 for tagged packets and a valid integer between 1518 - 9216 for untagged packets.

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 673.

Default	1518 (untagged)
Format	`mtu` *`size`*
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)

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

This command disables all ports.

Note: 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

Use this command to enable or disable auto-negotiation and set the speed that will be advertised by that port. 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. Use the command without the `auto` keyword to ensure auto-negotiation is disabled and to set the port speed and mode according to the command values. If auto-negotiation is disabled, the speed and duplex mode must be set.

Default	Auto-negotiation is enabled.
Format	`speed {auto {40G | 10G | 1000 | 100 | 10} [40G | 10G | 1000 | 100 | 10] [half-duplex | full-duplex] | {40G | 10G | 1000 | 100 | 10} {half-duplex | full-duplex}}`
Mode	Interface Config

speed all

This command sets the speed and duplex setting for all interfaces.

Format	`speed all {100 | 10} {half-duplex | full-duplex}`
Mode	Global Config

show port

This command displays port information.

Format	`show port {`*`intf-range`*` | 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** — this port is a monitoring port. For more information, see *Port Mirroring Commands* on page 509. • **PC Mbr**— this port is a member of a port-channel (LAG). • **Probe** — this 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

                 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
```

show port advertise

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, phy supervisor/member clock 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.

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

This command displays the interface description. 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 description [`*unit/slot/port* `|` `lag` *lag-intf-num*`]`
Mode	Privileged EXEC

Term	Definition
Interface	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 358.

Term	Definition
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
```

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

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

Use this command to allow the interface to become an edge port if it does not receive any BPDUs within a given amount of time.

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

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	`spanning-tree backbonefast`
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	`no spanning-tree backbonefast`
Mode	Global Config

spanning-tree bpdufilter

Use this command to enable BPDU Filter on an interface or range of interfaces.

Default	disabled
Format	`spanning-tree bpdufilter`
Mode	Interface Config

no spanning-tree bpdufilter

Use this command to disable BPDU Filter on the interface or range of interfaces.

Default	disabled
Format	`no spanning-tree bpdufilter`
Mode	Interface Config

spanning-tree bpdufilter default

Use this command to enable BPDU Filter on all the edge port interfaces.

Default	disabled
Format	`spanning-tree bpdufilter default`
Mode	Global Config

no spanning-tree bpdufilter default

Use this command to disable BPDU Filter on all the edge port interfaces.

Default	disabled
Format	`no spanning-tree bpdufilter default`
Mode	Global Config

spanning-tree bpduflood

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

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

Use this command to force a transmission of rapid spanning tree (RSTP) and multiple spanning tree (MSTP) BPDUs. Use the *`unit/slot/port`* parameter to transmit a BPDU from a specified interface, or use the **`all`** 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.

Format	`spanning-tree bpdumigrationcheck {`*`unit/slot/port`* `| all}`
Mode	Global Config

spanning-tree configuration name

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	`spanning-tree configuration name` *`name`*
Mode	Global Config

no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format	`no spanning-tree configuration name`
Mode	Global Config

spanning-tree configuration revision

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	`spanning-tree configuration revision` *number*
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	`no spanning-tree configuration revision`
Mode	Global Config

spanning-tree cost

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	`spanning-tree cost {`*`cost`*` | auto}`
Mode	Interface Config

no spanning-tree cost

This command resets the auto-edge status of the port to the default value.

Format	`no spanning-tree cost`
Mode	Interface Config

spanning-tree edgeport

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	`spanning-tree edgeport`
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	`no spanning-tree edgeport`
Mode	Interface Config

spanning-tree forward-time

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 “(Bridge Max Age / 2) + 1”.

Default	15
Format	`spanning-tree forward-time` *`value`*
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	`no spanning-tree forward-time`
Mode	Global Config

spanning-tree guard

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

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 x (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

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	`spanning-tree max-hops` *`value`*
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	`no spanning-tree max-hops`
Mode	Global Config

spanning-tree mode

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 reenable 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	`spanning-tree mode {mst | pvst | rapid-pvst | rstp | stp}`
Mode	Global Config

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. 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	cost—auto port-priority—128
Format	`spanning-tree mst` *`mstid`* `{{cost` *`number`* `| auto} | port-priority` *`number`*`}`
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	`no spanning-tree mst` *mstid* `{cost | port-priority}`
Mode	Interface Config

spanning-tree mst instance

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	`spanning-tree mst instance` *mstid*
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	`no spanning-tree mst instance` *mstid*
Mode	Global Config

spanning-tree mst priority

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	`spanning-tree mst priority` *`mstid value`*
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	`no spanning-tree mst priority` *`mstid`*
Mode	Global Config

spanning-tree mst vlan

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	`spanning-tree mst vlan` *`mstid vlanid`*
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	`no spanning-tree mst vlan` *`mstid vlanid`*
Mode	Global Config

spanning-tree port mode

This command sets the Administrative Switch Port State for this 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 this 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

This command sets the Administrative Switch Port State for all ports to enabled.

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.

Format	`no spanning-tree port mode all`
Mode	Global Config

spanning-tree port-priority

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	`spanning-tree port-priority` *`value`*
Mode	Interface Config

spanning-tree tcnguard

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	`spanning-tree tcnguard`
Mode	Interface Config

no spanning-tree tcnguard

This command resets the TCN guard status of the port to the default value.

Format	`no spanning-tree tcnguard`
Mode	Interface Config

spanning-tree transmit

This command sets the Bridge Transmit Hold Count parameter.

Default	6
Format	`spanning-tree transmit` *`hold-count`*
Mode	Global Config

Parameter	Description
hold-count	The Bridge Tx hold-count parameter. The value in an integer between 1 and 10.

spanning-tree uplinkfast

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 fowarding 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	`spanning-tree uplinkfast [max-update-rate` *`packets`*`]`
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	`no spanning-tree uplinkfast [max-update-rate]`
Mode	Global Config

spanning-tree vlan

Use this command to enable/disable spanning tree on a VLAN.

Default	`None`
Format	`spanning-tree vlan` *`vlan-list`*
Mode	Global Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.

spanning-tree vlan cost

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	`spanning-tree vlan` *`vlan-id`* `cost {auto |` *`value`*`}`
Mode	Interface Config

spanning-tree vlan forward-time

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. The network operator should 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	`spanning-tree vlan` *`vlan-list`* `forward-time` *`seconds`*
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.

spanning-tree vlan hello-time

Use this command to configure the spanning tree hello time for a specified VLAN or a range 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` *`vlan-list`* `hello-time` *`seconds`*
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.

spanning-tree vlan max-age

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	`spanning-tree vlan` *`vlan-list`* `max-age` *`seconds`*
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.

spanning-tree vlan root

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	`spanning-tree vlan` *`vlan-list`* `root {primary | secondary}`
Mode	Global Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.

spanning-tree vlan port-priority

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	`spanning-tree vlan` *`vlan-id`* `port-priority` *`priority`*
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.

spanning-tree vlan priority

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	`spanning-tree vlan` *`vlan-list`* `priority` *`priority`*
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.

show spanning-tree

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.

Term	Definition
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).
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 Routing) #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 backbonefast

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

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 Routing) #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

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. 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. The following details are displayed on execution of the command.

Format	`show spanning-tree interface [`*unit/slot/port* `|` `lag` *lag-intf-num*`]`
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.

Term	Definition
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.
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 Routing) >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 Routing) >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

This command displays the detailed settings for an MST instance.

Format	`show spanning-tree mst detailed` *mstid*
Mode	Privileged EXEC User EXEC

Parameter	Description
mstid	A multiple spanning tree instance identifier. The value is 0–4094.

Command example:

```
(NETGEAR Routing) >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

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. The *unit/slot/port* is the desired switch port. 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 spanning-tree mst port detailed` *mstid* [*unit/slot/port* | `lag` *lag-intf-num*]
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.

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 slot/port format:

```
(NETGEAR Routing) >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 Routing) >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

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. The parameter *unit/slot/port* indicates the desired switch port; the keyword **all** indicates all ports. 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.

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	`show spanning-tree mst port summary` *mstid* {*unit/slot/port* | lag *lag-intf-num* | all}
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.

Term	Definition
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 slot/port format:

```
(NETGEAR Routing) >show spanning-tree mst port summary 0 0/1

MST Instance ID.............................. CST

            STP                  STP            Port
Interface   Mode   Type         State          Role       Desc
--------- -------- ------- ----------------- ---------- ----------
0/1       Enabled          Disabled          Disabled
```

Command example:

The following example shows output using a LAG interface number:

```
(NETGEAR Routing) >show spanning-tree mst port summary 0 lag 1

MST Instance ID.............................. CST

            STP                  STP            Port
Interface   Mode   Type         State          Role       Desc
--------- -------- ------- ----------------- ---------- ----------
3/1       Enabled          Disabled          Disabled
```

show spanning-tree mst port summary active

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` *`mstid`* `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.

Term	Definition
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 Routing) >show spanning-tree mst port summary 0 active

            STP                  STP            Port
Interface   Mode   Type         State           Role       Desc
--------- -------- ------- ----------------- ---------- ---------
```

show spanning-tree mst summary

This command displays summary information about all multiple spanning tree instances in the switch. On execution, the following details are displayed.

Format	`show spanning-tree mst summary`
Mode	Privileged EXEC User EXEC

Term	Definition
MST Instance ID List	List of multiple spanning trees IDs currently configured.
For each MSTID: Associated FIDs Associated VLANs	List of forwarding database identifiers associated with this instance. List of VLAN IDs associated with this instance.

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 Routing) >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

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

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* 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
```

VLAN Commands

This section describes the commands you use to configure VLAN settings.

vlan database

This command gives you access to the VLAN Config mode, which allows you to configure VLAN characteristics.

Format	`vlan database`
Mode	Privileged EXEC

network mgmt_vlan

This command configures the Management VLAN ID, which can be a VLAN number in the range 1–4093.

Default	1
Format	`network mgmt_vlan` *number*
Mode	Privileged EXEC

no network mgmt_vlan

This command sets the Management VLAN ID to the default.

Format	`no network mgmt_vlan`
Mode	Privileged EXEC

vlan

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` *`number`*
Mode	VLAN 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	`no vlan` *`number`*
Mode	VLAN Config

vlan acceptframe

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	`vlan acceptframe {admituntaggedonly | vlanonly | all}`
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	`no vlan acceptframe`
Mode	Interface Config

vlan ingressfilter

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	`vlan ingressfilter`
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	`no vlan ingressfilter`
Mode	Interface Config

vlan internal allocation

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	`vlan internal allocation {base` *`vlan-id`* `| policy ascending | policy decending}`
Mode	Global Config

Parameter	Description
base *vlan-id*	The first VLAN ID to be assigned to a port-based routing interface.
policy ascending	VLAN IDs assigned to port-based routing interfaces start at the base and increase in value
policy descending	VLAN IDs assigned to port-based routing interfaces start at the base and decrease in value

vlan makestatic

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	`vlan makestatic` *`number`*
Mode	VLAN Config

vlan name

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	`vlan name` *`number name`*
Mode	VLAN Config

no vlan name

This command sets the name of a VLAN to a blank string.

Format	`no vlan name` *`number`*
Mode	VLAN Config

vlan participation

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	`vlan participation {exclude | include | auto}` *`number`*
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.

vlan participation all

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	`vlan participation all {exclude | include | auto}` *`number`*
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.

vlan port acceptframe all

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

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

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` *number*
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

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` *`number`*
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` *`number`*
Mode	Global Config

vlan protocol group

This command adds protocol-based VLAN groups to the system. The *`groupid`* is a unique number from 1–128 that is used to identify the group in subsequent commands.

Format	`vlan protocol group` *`groupid`*
Mode	Global Config

vlan protocol group name

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` *`groupid groupname`*
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` *`groupid`*
Mode	Global Config

vlan protocol group add protocol

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	`vlan protocol group add protocol` *`groupid ethertype protocol-list`*
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	`no vlan protocol group add protocol` *`groupid ethertype protocol-list`*
Mode	Global Config

protocol group

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	`protocol group` *`groupid vlanid`*
Mode	VLAN Config

no protocol group

This command removes the *`vlanid`* from this protocol-based VLAN group that is identified by this *`groupid`*.

Format	`no protocol group` *`groupid vlanid`*
Mode	VLAN Config

protocol vlan group

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 groupid`
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 groupid`
Mode	Interface Config

protocol vlan group all

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 groupid`
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 groupid`
Mode	Global Config

show port protocol

This command displays the Protocol-Based VLAN information for either the entire system, or for the indicated group.

Format	`show port protocol {groupid | 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 *unit/slot/port* interface(s) that are associated with this Protocol Group.

vlan pvid

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` *number*
Mode	Interface Config Interface Range 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

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` *number*
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` *number*
Mode	Interface Config

vlan association subnet

This command associates a VLAN to a specific IP-subnet.

Format	`vlan association subnet` *`ipaddr netmask vlanid`*
Mode	VLAN Config

no vlan association subnet

This command removes association of a specific IP-subnet to a VLAN.

Format	`no vlan association subnet` *`ipaddr netmask`*
Mode	VLAN Config

vlan association mac

This command associates a MAC address to a VLAN.

Format	`vlan association mac` *`macaddr vlanid`*
Mode	VLAN database

no vlan association mac

This command removes the association of a MAC address to a VLAN.

Format	`no vlan association mac` *`macaddr`*
Mode	VLAN database

remote-span

This command identifies the VLAN as the RSPAN VLAN.

Default	`None`
Format	`remote-span`
Mode	VLAN configuration

show vlan

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	`show vlan {`*`vlan-id`*` | private-vlan [`*`type`*`]}`
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.
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

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

This command displays VLAN port information.

Format	`show vlan port {`*`unit/slot/port`*` | all}`
Mode	Privileged EXEC User EXEC

Term	Definition
Interface	It is possible to set the parameters for all ports by using the selectors on the top line.
Port VLAN ID	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

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 [ipaddr netmask]`
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

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 [macaddr]`
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.

Switch Port Commands

This section describes the commands used for switch port mode.

switchport mode

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	`switchport mode {access | trunk | general}`
Mode	Interface Config

no switchport mode

This command resets the switch port mode to its default value.

Format	`no switchport mode`
Mode	Interface Config

switchport trunk allowed vlan

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	`all`
Format	`switchport trunk allowed vlan {`*`vlan-list`*` | all | {add `*`vlan-list`*`} | {remove `*`vlan-list`*`} | {except `*`vlan-list`*`}}`
Mode	Interface Config

Parameter	Description
`all`	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.
`add`	Adds the defined list of VLANs to those currently set instead of replacing the list.

Parameter	Description
`remove`	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
`except`	Lists the VLANs that must be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.)
`van-list`	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 vlan

This command resets the list of allowed VLANs on the trunk port to its default value.

Format	`no switchport trunk allowed vlan`
Mode	Interface Config

switchport trunk native vlan

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	`switchport trunk native vlan` *`vlan-id`*
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	`no switchport trunk native vlan`
Mode	Interface Config

switchport access vlan

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	`switchport access vlan` *`vlan-id`*
Mode	Interface Config

no switchport access vlan

This command resets the switch port access mode VLAN to its default value.

Format	`no switchport access vlan`
Mode	Interface Config

show interfaces switchport

Use this command to either display the switch port status for all interfaces, for a specific interface, or for a specific mode (access, trunk, or general). If you select a mode but do not specify the interface for the mode, the selected mode is displayed for all interfaces.

Format	`show interfaces switchport {[`*`unit/slot/port`*`] | {access | trunk | general} [`*`unit/slot/port`*`]}`
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    Acceptable  Untagged  Tagged    Forbidden Dynamic
                Filtering  Frame Type  Vlans     Vlans     Vlans     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    Acceptable  Untagged  Tagged    Forbidden Dynamic
                Filtering  Frame Type  Vlans     Vlans     Vlans     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 (Interface Config)

This command configures the ethertype for the 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	`dvlan-tunnel ethertype {802.1Q | vman | custom` *value*`}`
Mode	Global 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 (Interface Config)

This command removes the ethertype value for the interface.

Format	`no dvlan-tunnel ethertype`
Mode	Global Config

dvlan-tunnel ethertype primary-tpid

Use this command to create a new TPID and associate it with the next available TPID register. If no TPID registers are empty, the system returns an error. Specifying the optional keyword **primary-tpid** forces the TPID value to be configured as the default TPID at index 0. 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.

Format	`dvlan-tunnel ethertype {802.1Q | vman | custom` *value*`} [primary-tpid]`
Mode	Global Config

Parameter	Description
802.1Q	Configure the ethertype as 0x8100.
custom value	Configure the value of the custom tag in the range from 1 to 65535.
vman	Represents the commonly used value of 0x88A8.
primary-tpid	[Optional] Forces the TPID value to be configured as the default TPID at index 0.

no dvlan-tunnel ethertype primary–tpid

Use the no form of the command to reset the TPID register to 0. (At initialization, all TPID registers will be set to their default values.)

Format	`no dvlan-tunnel ethertype {802.1Q | vman | custom` *`1–65535`*`} [primary-tpid]`
Mode	Global Config

mode dot1q-tunnel

This command is used to enable Double VLAN Tunneling on the specified interface.

Default	disabled
Format	`mode dot1q-tunnel`
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	`no mode dot1q-tunnel`
Mode	Interface Config

mode dvlan-tunnel

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

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 or all interfaces.

Format	`show dot1q-tunnel [interface {`*`unit/slot/port`*` | all}]`
Mode	Privileged EXEC User EXEC

Term	Definition
Interface	The interface.
Mode	The administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.
EtherType	A 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. There are three different EtherType tags. The first is 802.1Q, which represents the commonly used value of 0x8100. The second is vMAN, which represents the commonly used value of 0x88A8. If EtherType is not one of these two values, then it is a custom tunnel value, representing any value in the range of 1 to 65535.

show dvlan-tunnel

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 or all interfaces.

Format	`show dvlan-tunnel [interface {`*`unit/slot/port`*` | all | lag `*`lag-intf-num`*`}]`
Mode	Privileged EXEC User EXEC

Term	Definition
Interface	The interface.
LAG	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.
Mode	The administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.
EtherType	A 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. There are three different EtherType tags. The first is 802.1Q, which represents the commonly used value of 0x8100. The second is vMAN, which represents the commonly used value of 0x88A8. If EtherType is not one of these two values, then it is a custom tunnel value, representing any value in the range of 1 to 65535.

Command example:

```
(NETGEAR Switch) #show dvlan-tunnel

TPIDs Configured.............................. 0x88a8
Default TPID.................................. 0x88a8
Interfaces Enabled for DVLAN Tunneling......... None

(NETGEAR Routing) #

(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

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` *primary-vlan-id secondary-vlan-id* `| mapping` *primary-vlan-id* `{add | remove}` *secondary-vlan-list*`}`
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.
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.

no switchport private-vlan

This command removes the private-VLAN association or mapping from the port.

Format	`no switchport private-vlan {host-association | mapping}`
Mode	Interface Config

switchport mode private-vlan

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}`
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.

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

This command configures the private VLANs and configures the association between the primary private VLAN and secondary VLANs.

Format	`private-vlan {association [add | remove] secondary-vlan-list | community | isolated | primary}`
Mode	VLAN Config

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	`no private-vlan [association]`
Mode	VLAN Config

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 given 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, then the priority info 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 given 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 given 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.

When a dot1p priority is configured on the voice VLAN port instead of VLAN ID, then the priority information is passed onto the VoIP phone using the LLDP-MED mechanism. 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 given the default priority of the port (default 0), and the voice traffic is received with higher priority, 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.

Note: The IP phone must support LLDP-MED to accept the VLAN ID and CoS information from the switch.

voice vlan (Global Config)

Use this command to enable the Voice VLAN capability on the switch.

Default	disabled
Format	`voice vlan`
Mode	Global Config

no voice vlan (Global Config)

Use this command to disable the Voice VLAN capability on the switch.

Format	`no voice vlan`
Mode	Global Config

voice vlan (Interface Config)

Use this command to enable the Voice VLAN capability on the interface or range of interfaces.

Default	disabled
Format	`voice vlan {`*`vlan-id`*` | dot1p `*`priority`*` | none | untagged}`
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	`no voice vlan`
Mode	Interface Config

voice vlan data priority

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

show voice vlan

Use this command to display information about the voice VLAN.

Format	`show voice vlan [interface {`*`unit/slot/port`*` | all}]`
Mode	Privileged EXEC

When the **`interface`** parameter is not specified, only the global mode of the Voice VLAN is displayed.

Term	Definition
Administrative Mode	The Global Voice VLAN mode.

When the **`interface`** parameter is specified..

Term	Definition
Voice VLAN Mode	The admin mode of the Voice VLAN on the interface.
Voice VLAN ID	The Voice VLAN ID
Voice VLAN Priority	The do1p priority for the Voice VLAN on the port.
Voice VLAN Untagged	The tagging option for the Voice VLAN traffic.
Voice VLAN CoS Override	The Override option for the voice traffic arriving on the port.
Voice VLAN Status	The operational status of Voice VLAN on the port.

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

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` *priority*
Mode	Global Config

vlan priority

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` *priority*
Mode	Interface Config

Asymmetric Flow Control

Note: Asymmetric Flow Control is not supported on Fast Ethernet platforms.

Note: If Asymmetric Flow Control is not supported on the platform, then only symmetric, or no flow control, modes are configurable.

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

Note: The **flowcontrol** command is available if the platform supports only the symmetric flow control feature.

Use this command to enable or disable the symmetric flow control on the switch.

Default	Flow control is disabled.
Format	flowcontrol
Mode	Global Config

no flowcontrol

This command disables the symmetric flow control.

Format	no flowcontrol
Mode	Global Config

show flowcontrol

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 chassis ports is always displayed as N/A.

Format	show flowcontrol [interface *unit/slot/port*]
Mode	Privileged Exec

Command example:

```
(NETGEAR Switch)#show flowcontrol

Admin Flow Control: Symmetric

Port     Flow Control     RxPause     TxPause
         Oper
------   ------------     --------    ---------
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  RxPause      TxPause
           Oper
---------  -------       --------     -------
0/1        Active        310          611
```

Protected Ports 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)

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` *groupid* `name` *name*
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` *groupid* `name` *name*
Mode	Global Config

switchport protected (Interface Config)

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	`switchport protected` *groupid*
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	`no switchport protected` *groupid*
Mode	Interface Config

show switchport protected

This command displays the status of all the interfaces, including protected and unprotected interfaces.

Format	`show switchport protected` *groupid*
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 *groupid*. If no port is configured as protected for this group, this field is blank.

show interfaces switchport (for a group ID)

This command displays the status of the interface (protected or unprotected) under the *groupid*.

Format	`show interfaces switchport` *unit/slot/port groupid*
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 *groupid*.

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

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	`switchport private-group [`*`privategroup-name`*` | `*`privategroup-id`*`]`
Mode	Interface Config

no switchport private-group

This command removes a port from to a private group.

Format	`no switchport private-group [`*`privategroup-name`*` | `*`privategroup-id`*`]`
Mode	Interface Config

private-group name

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	`private-group name `*`privategroup-name`*` [`*`private-group-id`*`] [mode {community | isolated}]`
Mode	Global Config

no private-group name

This command removes a private group.

Format	`no private-group name `*`privategroup-name`*
Mode	Global Config

show private-group

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.

Format	`show private-group [`*`private-group-name`*` | `*`private-group-id`*` | port `*`unit/slot/port`*`]`
Mode	Privileged EXEC

Term	Description
Interface	A valid slot and port number separated by forward slashes.
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

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	`set garp timer join` *`centiseconds`*
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	`no set garp timer join`
Mode	Interface Config Global Config

set garp timer leave

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 unregister 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	`set garp timer leave` *`centiseconds`*
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	`no set garp timer leave`
Mode	Interface Config Global Config

set garp timer leaveall

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	`set garp timer leaveall` *`centiseconds`*
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

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

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

This command enables GVRP on a single port (Interface Config mode), a range of ports (Interface Range mode), or all ports (Global Config mode).

Default	disabled
Format	`set gvrp interfacemode`
Mode	Interface Config Interface Range 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

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format	`show gvrp configuration {`*`unit/slot/port`*` | all}`
Mode	Privileged EXEC User EXEC

Term	Definition
Interface	*unit/slot/port*
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).

Term	Definition
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

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

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

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format	`show gmrp configuration {`*`unit/slot/port`*` | all}`
Mode	Privileged EXEC User EXEC

Term	Definition
Interface	The *`unit/slot/port`* 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).

Term	Definition
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. 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

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). 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

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.
- **local**. Uses the local user name 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. However, you can configure more than one method by issuing the command several times.

Format	`aaa authentication dot1x default {ias | local | none | radius}`
Mode	Global Config

Command example:

```
(NETGEAR Routing) #
(NETGEAR Routing) #configure
(NETGEAR Routing) (Config)#aaa authentication dot1x default ias
(NETGEAR Routing) (Config)#aaa authentication dot1x default local
```

clear dot1x statistics

This command resets the 802.1X statistics for the specified port or for all ports.

Format	`clear dot1x statistics {`*`unit/slot/port`*` | all}`
Mode	Privileged EXEC

clear dot1x authentication-history

This command clears the authentication history table captured during successful and unsuccessful authentication on all interface or the specified interface.

Format	`clear dot1x authentication-history [`*`unit/slot/port`*`]`
Mode	Privileged EXEC

clear radius statistics

This command is used to clear all RADIUS statistics.

Format	`clear radius statistics`
Mode	Privileged EXEC

dot1x eapolflood

Use this command to enable EAPOL flood support on the switch.

Default	disabled
Format	`dot1x eapolflood`
Mode	Global Config

no dot1x eapolflood

This command disables EAPOL flooding on the switch.

Format	`no dot1x eapolflood`
Mode	Global Config

dot1x dynamic-vlan enable

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	`dot1x dynamic-vlan enable`
Mode	Global Config

no dot1x 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	`no dot1x dynamic-vlan enable`
Mode	Global Config

dot1x guest-vlan

This command configures VLAN as guest vlan on an interface or a range of interfaces. The command specifies an active VLAN as an IEEE 802.1X guest VLAN. The range is 1 to the maximum VLAN ID supported by the platform.

Default	disabled
Format	`dot1x guest-vlan` *`vlan-id`*
Mode	Interface Config

no dot1x guest-vlan

This command disables Guest VLAN on the interface.

Default	disabled
Format	`no dot1x guest-vlan`
Mode	Interface Config

dot1x initialize

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is auto or mac-based. If the control mode is not auto or mac-based, an error is returned.

Format	`dot1x initialize` *`unit/slot/port`*
Mode	Privileged EXEC

dot1x max-req

This command sets the maximum number of times the authenticator state machine on an interface or range of interfaces will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant. The *`count`* parameter must be in the range 1–10.

Default	2
Format	`dot1x max-req` *`count`*
Mode	Interface Config

no dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Format	`no dot1x max-req`
Mode	Interface Config

dot1x max-users

Use this command to set the maximum number of clients supported on an interface or range of interfaces when MAC-based dot1x authentication is enabled on the port. The maximum users supported per port is dependent on the product. The *`count`* parameter must be in the range 1–48.

Default	48
Format	`dot1x max-users` *`count`*
Mode	Interface Config

no dot1x max-users

This command resets the maximum number of clients allowed per port to its default value.

Format	`no dot1x max-users`
Mode	Interface Config

dot1x port-control

This command sets the authentication mode to use on the specified interface or range of interfaces. Use the **`force-unauthorized`** parameter to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Use the **`force-authorized`** parameter to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Use the **`auto`** 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. If the **`mac-based`** parameter is specified, then MAC-based dot1x authentication is enabled on the port.

Default	`auto`
Format	`dot1x port-control {force-unauthorized | force-authorized | auto | mac-based}`
Mode	Interface Config

no dot1x port-control

This command sets the 802.1X port control mode on the specified port to the default value.

Format	`no dot1x port-control`
Mode	Interface Config

dot1x port-control all

This command sets the authentication mode to use on all ports. Select the **`force-unauthorized`** parameter to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select the **`force-authorized`** parameter to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select the **`auto`** 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. If the **`mac-based`** parameter is specified, then MAC-based dot1x authentication is enabled on the port.

Default	auto
Format	`dot1x port-control all {force-unauthorized | force-authorized | auto | mac-based}`
Mode	Global Config

no dot1x port-control all

This command sets the authentication mode on all ports to the default value.

Format	`no dot1x port-control all`
Mode	Global Config

dot1x mac-auth-bypass

If the 802.1X mode on the interface is mac-based, you can optionally 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.

Default	disabled
Format	`dot1x mac-auth-bypass`
Mode	Interface Config

no dot1x mac-auth-bypass

This command sets the MAB mode on the ports to the default value.

Format	`no dot1x mac-auth-bypass`
Mode	Interface Config

dot1x re-authenticate

This command begins the reauthentication sequence on the specified port. This command is only valid if the control mode for the specified port is auto or mac-based. If the control mode is not auto or mac-based, an error is returned.

Format	`dot1x re-authenticate` *`unit/slot/port`*
Mode	Privileged EXEC

dot1x re-authentication

This command enables reauthentication of the supplicant for the specified interface or range of interfaces.

Default	disabled
Format	`dot1x re-authentication`
Mode	Interface Config

no dot1x re-authentication

This command disables reauthentication of the supplicant for the specified port.

Format	`no dot1x re-authentication`
Mode	Interface Config

dot1x system-auth-control

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	`dot1x system-auth-control`
Mode	Global Config

no dot1x system-auth-control

This command is used to disable the dot1x authentication support on the switch.

Format	`no dot1x system-auth-control`
Mode	Global Config

dot1x system-auth-control monitor

Use this command to enable the 802.1X monitor mode on the switch. The purpose of Monitor mode is to help troubleshoot port-based authentication configuration issues without disrupting network access for hosts connected to the switch. In Monitor mode, a host is granted network access to an 802.1X-enabled port even if it fails the authentication process. The results of the process are logged for diagnostic purposes.

Default	disabled
Format	`dot1x system-auth-control monitor`
Mode	Global Config

no dot1x system-auth-control monitor

This command disables the 802.1X Monitor mode on the switch.

Format	`no dot1x system-auth-control monitor`
Mode	Global Config

dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on an interface or range of interfaces. Depending on the token used and the value (in seconds) passed, various timeout configurable parameters are set. The following tokens are supported:

Tokens	Definition
guest-vlan-period	The time, in seconds, for which the authenticator waits to see if any EAPOL packets are received on a port before authorizing the port and placing the port in the guest vlan (if configured). The guest vlan timer is only relevant when guest vlan has been configured on that specific port.
reauth-period	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.
quiet-period	The value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet-period must be a value in the range 0 - 65535.
tx-period	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The quiet-period must be a value in the range 1 - 65535.
supp-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supp-timeout must be a value in the range 1 - 65535.
server-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The supp-timeout must be a value in the range 1 - 65535.

Default	guest-vlan-period: 90 seconds reauth-period: 3600 seconds quiet-period: 60 seconds tx-period: 30 seconds supp-timeout: 30 seconds server-timeout: 30 seconds
Format	`dot1x timeout {{guest-vlan-period` *`seconds`*`} |{reauth-period` *`seconds`*`} | {quiet-period` *`seconds`*`} | {tx-period` *`seconds`*`} | {supp-timeout` *`seconds`*`} | {server-timeout` *`seconds`*`}}`
Mode	Interface Config

no dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to the default values. Depending on the token used, the corresponding default values are set.

Format	`no dot1x timeout {guest-vlan-period | reauth-period | quiet-period | tx-period | supp-timeout | server-timeout}`
Mode	Interface Config

dot1x unauthenticated-vlan

Use this command to configure the unauthenticated VLAN associated with the specified interface or range of interfaces. The unauthenticated VLAN ID can be a valid VLAN ID from 0–maximum supported VLAN ID (4093 for NETGEAR Managed Switch). The unauthenticated VLAN must be statically configured in the VLAN database to be operational. By default, the unauthenticated VLAN is 0, i.e. invalid and not operational.

Default	0
Format	`dot1x unauthenticated-vlan` *`vlan-id`*
Mode	Interface Config

no dot1x unauthenticated-vlan

This command resets the unauthenticated-vlan associated with the port to its default value.

Format	`no dot1x unauthenticated-vlan`
Mode	Interface Config

dot1x user

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.

Format	`dot1x user` *`user`* `{`*`unit/slot/port`* `| all}`
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	`no dot1x user` *`user`* `{`*`unit/slot/port`* `| all}`
Mode	Global Config

authentication enable

This command globally enables the Authentication Manager. Interface configuration takes effect only if the Authentication Manager is enabled with this command.

Note: The Authentication Manager is supported on M6100 series switches only.

Default	disabled
Format	`authentication enable`
Mode	Global Config

no authentication enable

This command disables the Authentication Manager.

Format	`no authentication enable`
Mode	Global Config

authentication order

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.

Note: This command is supported on M6100 series switches only.

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

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 decides if a previously authenticated client is reauthenticated with a higher-priority method when the same is received. Captive portal is always the last method in the list.

Note: This command is supported on M6100 series switches only.

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

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.

Note: This command is supported on M6100 series switches only.

Format	`authentication restart` *seconds*
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

show authentication authentication-history

Use this command to display information about the authentication history for a specified interface.

Note: This command is supported on M6100 series switches only.

Format	`show authentication authentication-history` *`unit/slot/port`*
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 Method	The authentication method and status for the interface.

Command example:

```
Time Stamp            Interface MAC-Address     Auth Status  Method
--------------------- --------- ----------------- ------ ------------
Jul 21 1919 15:06:15  1/0/1     00:00:00:00:00:01 Authorized  802.1X
```

show authentication interface

Use this command to display authentication method information either for all interfaces or a specified port.

Note: This command is supported on M6100 series switches only.

Format	`show authentication interface {all |` *`unit/slot/port`*`}`
Mode	Privileged EXEC

The following information is displayed for each interface.

Term	Definition
Interface	The interface for which authentication configuration information is being displayed.
Authentication Restart timer	The time, in seconds, after which reauthentication starts.
Configured method order	The order of authentication methods used on a port.

Term	Definition
Enabled method order	The order of authentication methods used on a port.
Configured method priority	The priority for the authentication methods used on a port.
Enabled method priority	The priority for the authentication methods used on a port.
Number of authenticated clients	The number of authenticated clients.
Logical Interface	The logical interface
Client MAC addr	The MAC address for the client.
Authenticated Method	The current authentication method.
Auth State	If the authentication was successful.
Auth Status	The current authentication status.

Command example:

```
(NETGEAR Switch) #show authentication interface all

Interface..................................... 1/0/1
Authentication Restart timer.................. 300
Configured method order....................... dot1x mab captive-portal
Enabled method order.......................... dot1x mab undefined
Configured method priority.................... undefined undefined undefined
Enabled method priority....................... undefined undefined undefined
Number of authenticated clients............... 0
Interface..................................... 1/0/2
Authentication Restart timer.................. 300
Configured method order....................... dot1x mab captive-portal
Enabled method order.......................... dot1x mab undefined
Configured method priority.................... undefined undefined undefined
Enabled method priority....................... undefined undefined undefined
Number of authenticated clients............... 0
Interface..................................... 1/0/3
Authentication Restart timer.................. 300
Configured method order....................... dot1x mab captive-portal
Enabled method order.......................... dot1x mab undefined
Configured method priority.................... undefined undefined undefined
Enabled method priority....................... undefined undefined undefined
Number of authenticated clients............... 0
Interface..................................... 1/0/4
Authentication Restart timer.................. 300
Configured method order....................... dot1x mab captive-portal
Enabled method order.......................... dot1x mab undefined
Configured method priority.................... undefined undefined undefined
Enabled method priority....................... undefined undefined undefined
```

```
Number of authenticated clients.............. 0
```

show authentication methods

Use this command to display information about the authentication methods.

Note: This command is supported on M6100 series switches only.

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          enableNetList
SSH      networkList          enableNetList

HTTPS       :local
HTTP        :local
DOT1X       :
```

show authentication statistics

Use this command to display the authentication statistics for an interface.

Note: This command is supported on M6100 series switches only.

Format	`show authentication statistics` *`unit/slot/port`*
Mode	Privileged EXEC

The following information is displayed for each interface.

Term	Definition
Port	The port for which information is being 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.
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 Routing) #show authentication statistics 1/0/1

Port..................................... 1/0/1
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
```

clear authentication statistics

Use this command to clear the authentication statistics on an interface.

Note: This command is supported on M6100 series switches only.

Format	`clear authentication statistics {`*`unit/slot/port`*`] | all}`
Mode	Privileged EXEC

clear authentication authentication-history

Use this command to clear the authentication history log for an interface.

Note: This command is supported on M6100 series switches only.

Format	`clear authentication authentication-history {`*`unit/slot/port`* `| all}`
Mode	Privileged EXEC

show dot1x

This command is used to show a summary of the global dot1x configuration, summary information of the dot1x configuration for a specified port or all ports, the detailed dot1x configuration for a specified port and the dot1x statistics for a specified port, depending on the tokens used.

Format	`show dot1x [{summary {`*`unit/slot/port`* `| all} | detail` *`unit/slot/port`* `| statistics` *`unit/slot/port`*`}]`
Mode	Privileged EXEC

If you do not use the optional parameters *`unit/slot/port`*, the command displays the global dot1x mode, the VLAN Assignment mode, and the Dynamic VLAN Creation mode.

Term	Definition
Administrative Mode	Indicates whether authentication control on the switch is enabled or disabled.
VLAN Assignment Mode	Indicates whether assignment of an authorized port to a RADIUS-assigned VLAN is allowed (enabled) or not (disabled).
Dynamic VLAN Creation Mode	Indicates whether the switch can dynamically create a RADIUS-assigned VLAN if it does not currently exist on the switch.
Monitor Mode	Indicates whether the Dot1x Monitor mode on the switch is enabled or disabled.

If you use the optional parameter **`summary {`***`unit/slot/port`* **`| all}`**, the dot1x configuration for the specified port or all ports are displayed.

Term	Definition
Interface	The interface whose configuration is displayed.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized, force-authorized, auto, mac-based, authorized, and unauthorized.
Operating Control Mode	The control mode under which this port is operating. Possible values are authorized and unauthorized.
Reauthentication Enabled	Indicates whether reauthentication is enabled on this port.
Port Status	Indicates whether the port is authorized or unauthorized. Possible values are authorized and unauthorized.

Command example:

```
(NETGEAR Switch) #show dot1x summary 0/1
Operating
Interface       Control Mode       Control Mode       Port Status
---------       ------------       -----------        ------------
0/1             auto               auto               Authorized
```

If you use the optional parameter **`detail`** *`unit/slot/port`*, the detailed dot1x configuration for the specified port is displayed.

Term	Definition
Port	The interface whose configuration is displayed.
Protocol Version	The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.
PAE Capabilities	The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized, force-authorized, auto, and mac-based.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Quiet Period	The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0 and 65535.

Term	Definition
Transmit Period	The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Guest-VLAN ID	The guest VLAN identifier configured on the interface.
Guest VLAN Period	The time in seconds for which the authenticator waits before authorizing and placing the port in the Guest VLAN, if no EAPOL packets are detected on that port.
Supplicant Timeout	The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Server Timeout	The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1 and 65535.
Maximum Requests	The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of 1 and 10.
Configured MAB Mode	The administrative mode of the MAC authentication bypass feature on the switch.
Operational MAB Mode	The operational mode of the MAC authentication bypass feature on the switch. MAB might be administratively enabled but not operational if the control mode is not MAC based.
Vlan-ID	The VLAN assigned to the port by the radius server. This is only valid when the port control mode is not Mac-based.
VLAN Assigned Reason	The reason the VLAN identified in the VLAN-assigned field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Guest VLAN, default, and Not Assigned. When the VLAN Assigned Reason is Not Assigned, it means that the port has not been assigned to any VLAN by dot1x. This only valid when the port control mode is not MAC-based.
Reauthentication Period	The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1 and 65535.
Reauthentication Enabled	Indicates if reauthentication is enabled on this port. Possible values are True and False.
Key Transmission Enabled	Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.
EAPOL Flood Mode Enabled	Indicates whether the EAPOL flood support is enabled on the switch. Possible values are True and False.
Control Direction	The control direction for the specified port or ports. Possible values are both and in.
Maximum Users	The maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode. This value is used only when the port control mode is not MAC-based.
Unauthenticated VLAN ID	Indicates the unauthenticated VLAN configured for this port. This value is valid for the port only when the port control mode is not MAC-based.

Term	Definition
Session Timeout	Indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default, Radius-Request. If the value is Default, the session is terminated the port goes into unauthorized state. If the value is Radius-Request, then a reauthentication of the client authenticated on the port is performed. This value is valid for the port only when the port control mode is not MAC-based.

Command example:

```
(NETGEAR Switch) #show dot1x detail 1/0/3

Port..................................... 1/0/1
Protocol Version......................... 1
PAE Capabilities......................... Authenticator
Control Mode............................. auto
Authenticator PAE State.................. Initialize
Backend Authentication State............. Initialize
Quiet Period (secs)...................... 60
Transmit Period (secs)................... 30
Guest VLAN ID............................ 0
Guest VLAN Period (secs)................. 90
Supplicant Timeout (secs)................ 30
Server Timeout (secs).................... 30
Maximum Requests......................... 2
Configured MAB Mode...................... Enabled
Operational MAB Mode..................... Disabled
VLAN Id.................................. 0
VLAN Assigned Reason..................... Not Assigned
Reauthentication Period (secs)........... 3600
Reauthentication Enabled................. FALSE
Key Transmission Enabled................. FALSE
EAPOL flood Mode Enabled................. FALSE
Control Direction........................ both
Maximum Users............................ 16
Unauthenticated VLAN ID.................. 0
Session Timeout.......................... 0
Session Termination Action............... Default
```

For each client authenticated on the port, the **show dot1x detail** *unit/slot/port* command displays the following MAC-based dot1x parameters if the port-control mode for that specific port is MAC-based.

Term	Definition
Supplicant MAC-Address	The MAC-address of the supplicant.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.
VLAN-Assigned	The VLAN assigned to the client by the radius server.
Logical Port	The logical port number associated with the client.

If you use the optional parameter **statistics** *unit/slot/port*, the following dot1x statistics for the specified port appear.

Term	Definition
Port	The interface whose statistics are displayed.
EAPOL Frames Received	The number of valid EAPOL frames of any type that have been received by this authenticator.
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 EAPOL start frames that have been received by this authenticator.
EAPOL Logoff Frames Received	The number of EAPOL logoff frames that have been received by this authenticator.
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.
EAP Response/Id Frames Received	The number of EAP response/identity frames that have been received by this authenticator.
EAP Response Frames Received	The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.
EAP Request/Id Frames Transmitted	The number of EAP request/identity frames that have been transmitted by this authenticator.

Term	Definition
EAP Request Frames Transmitted	The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.
Invalid EAPOL Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EAP Length Error Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

show dot1x authentication-history

This command displays 802.1X authentication events and information during successful and unsuccessful Dot1x authentication process for all interfaces or the specified interface. Use the optional keywords to display only failure authentication events in summary or in detail.

Format	`show dot1x authentication-history {`*`unit/slot/port`*` | all} [failed-auth-only] [detail]`
Mode	Privileged EXEC

Term	Definition
Time Stamp	The exact time at which the event occurs.
Interface	Physical Port on which the event occurs.
Mac-Address	The supplicant/client MAC address.
VLAN assigned	The VLAN assigned to the client/port on authentication.
VLAN assigned Reason	The type of VLAN ID assigned, which can be Guest VLAN, Unauth, Default, RADIUS Assigned, or Monitor Mode VLAN ID.
Auth Status	The authentication status.
Reason	The actual reason behind the successful or failed authentication.

show dot1x clients

This command displays 802.1X client information. This command also displays information about the number of clients that are authenticated using Monitor mode and using 802.1X.

Format	`show dot1x clients {`*`unit/slot/port`*` | all}`
Mode	Privileged EXEC

Term	Definition
Clients Authenticated using Monitor Mode	Indicates the number of the Dot1x clients authenticated using Monitor mode.
Clients Authenticated using Dot1x	Indicates the number of Dot1x clients authenticated using 802.1x authentication process.
Logical Interface	The logical port number associated with a client.
Interface	The physical port to which the supplicant is associated.
User Name	The user name used by the client to authenticate to the server.
Supplicant MAC Address	The supplicant device MAC address.
Session Time	The time since the supplicant is logged on.
Filter ID	Identifies the Filter ID returned by the RADIUS server when the client was authenticated. This is a configured DiffServ policy name on the switch.
VLAN ID	The VLAN assigned to the port.
VLAN Assigned	The reason the VLAN identified in the VLAN ID field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Monitor Mode, or Default. When the VLAN Assigned reason is Default, it means that the VLAN was assigned to the port because the P-VID of the port was that VLAN ID.
Session Timeout	This value indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port-control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default and Radius-Request. If the value is Default, the session is terminated and client details are cleared. If the value is Radius-Request, then a reauthentication of the client is performed.

show dot1x users

This command displays 802.1X port security user information for locally configured users.

Format	`show dot1x users` *`unit/slot/port`*
Mode	Privileged EXEC

Term	Definition
Users	Users configured locally to have access to the specified port.

802.1X Supplicant Commands

NETGEAR Managed Switch supports 802.1X (dot1x) supplicant functionality on point-to-point ports. The administrator can configure the user name and password used in authentication and capabilities of the supplicant port.

dot1x pae

This command sets the port's dot1x role. The port can serve as either a supplicant or an authenticator.

Format	`dot1x pae {supplicant | authenticator}`
Mode	Interface Config

dot1x supplicant port-control

This command sets the ports authorization state (Authorized or Unauthorized) either manually or by setting the port to auto-authorize upon startup. By default all the ports are authenticators. If the port's attribute needs to be moved from authenticator to supplicant or from supplicant to authenticator, use this command.

Format	`dot1x supplicant port-control {auto | force-authorized | force-unauthorized}`
Mode	Interface Config

Parameter	Description
auto	The port is in the Unauthorized state until it presents its user name and password credentials to an authenticator. If the authenticator authorizes the port, then it is placed in the Authorized state.
force-authorized	Sets the authorization state of the port to Authorized, bypassing the authentication process.
force-unauthorized	Sets the authorization state of the port to Unauthorized, bypassing the authentication process.

no dot1x supplicant port-control

This command sets the port-control mode to the default, auto.

Default	auto
Format	`no dot1x supplicant port-control`
Mode	Interface Config

dot1x supplicant max-start

This command configures the number of attempts that the supplicant makes to find the authenticator before the supplicant assumes that there is no authenticator. The number of attempts can be in a range from 1–10. The default is 3 attempts.

Default	3
Format	`dot1x supplicant max-start` *number*
Mode	Interface Config

no dot1x supplicant max-start

This command sets the max-start value to the default.

Format	`no dot1x supplicant max-start`
Mode	Interface Config

dot1x supplicant timeout start-period

This command configures the start period timer interval to wait for the EAP identity request from the authenticator. The interval can be in a range from 1–65535 seconds. The default is 30 seconds.

Default	30 seconds
Format	`dot1x supplicant timeout start-period` *seconds*
Mode	Interface Config

no dot1x supplicant timeout start-period

This command sets the start-period value to the default.

Format	`no dot1x supplicant timeout start-period`
Mode	Interface Config

dot1x supplicant timeout held-period

This command configures the held period timer interval to wait for the next authentication on previous authentication fail. The interval can be in a range from 1–65535 seconds. The default is 30 seconds.

Default	60 seconds
Format	`dot1x supplicant timeout held-period` *seconds*
Mode	Interface Config

no dot1x supplicant timeout held-period

This command sets the held-period value to the default value.

Format	`no dot1x supplicant timeout held-period`
Mode	Interface Config

dot1x supplicant timeout auth-period

This command configures the authentication period timer interval to wait for the next EAP request challenge from the authenticator. The interval can be in a range from 1–65535 seconds. The default is 30 seconds.

Default	30 seconds
Format	`dot1x supplicant timeout auth-period` *seconds*
Mode	Interface Config

no dot1x supplicant timeout auth-period

This command sets the auth-period value to the default value.

Format	`no dot1x supplicant timeout auth-period`
Mode	Interface Config

dot1x supplicant user

Use this command to map the given user to the port.

Format	`dot1x supplicant user`
Mode	Interface Config

show dot1x statistics

This command displays the dot1x port statistics in detail.

Format	`show dot1x statistics` *unit/slot/port*
Mode	Privileged EXEC User EXEC

Term	Definition
EAPOL Frames Received	Displays the number of valid EAPOL frames received on the port.
EAPOL Frames Transmitted	Displays the number of EAPOL frames transmitted via the port.

Term	Definition
EAPOL Start Frames Transmitted	Displays the number of EAPOL Start frames transmitted via the port.
EAPOL Logoff Frames Received	Displays the number of EAPOL Log off frames that have been received on the port.
EAP Resp/ID Frames Received	Displays the number of EAP Respond ID frames that have been received on the port.
EAP Response Frames Received	Displays the number of valid EAP Respond frames received on the port.
EAP Req/ID Frames Transmitted	Displays the number of EAP Requested ID frames transmitted via the port.
EAP Req Frames Transmitted	Displays the number of EAP Request frames transmitted via the port.
Invalid EAPOL Frames Received	Displays the number of unrecognized EAPOL frames received on this port.
EAP Length Error Frames Received	Displays the number of EAPOL frames with an invalid Packet Body Length received on this port.
Last EAPOL Frames Version	Displays the protocol version number attached to the most recently received EAPOL frame.
Last EAPOL Frames Source	Displays the source MAC Address attached to 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
```

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.

NETGEAR Managed Switch provides broadcast, multicast, and unicast story 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 ingressing on 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 512bytes packets are used.

---

storm-control broadcast

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 ingressing on 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	disabled
Format	`storm-control broadcast`
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	`no storm-control broadcast`
Mode	Global Config Interface Config

storm-control broadcast level

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 ingressing on 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	`storm-control broadcast level` *`threshold`*
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

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 ingressing on 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 0–33554431. The default is 0.

Default	0
Format	`storm-control broadcast rate` *`threshold`*
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

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 ingressing on 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	`storm-control multicast`
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	`no storm-control multicast`
Mode	Global Config Interface Config

storm-control multicast level

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 ingressing on 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	`storm-control multicast level` *`0-100`*
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	`no storm-control multicast level`
Mode	Global Config Interface Config

storm-control multicast rate

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 ingressing on 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 0–33554431. The default is 0.

Default	0
Format	`storm-control multicast rate` *`threshold`*
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	`no storm-control multicast rate`
Mode	Global Config Interface Config

storm-control unicast

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 ingressing on 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	`storm-control unicast`
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	`no storm-control unicast`
Mode	Global Config Interface Config

storm-control unicast level

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 ingressing on 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	`storm-control unicast level` *`threshold`*
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	`no storm-control unicast level`
Mode	Global Config Interface Config

storm-control unicast rate

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 ingressing on 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 0–33554431. The default is 0.

Default	0
Format	`storm-control unicast rate` *`threshold`*
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	`no storm-control unicast rate`
Mode	Global Config Interface Config

show storm-control

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, or specify the *unit/slot/port* to display information about a specific interface.

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.
Mcast Mode	Shows whether the multicast storm control mode is enabled or disabled.
Mcast Level	The multicast storm control level.
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.

Command example:

```
(NETGEAR Switch) #show storm-control

Broadcast Storm Control Mode.................. Disable
Broadcast Storm Control Level................. 5 percent
Multicast Storm Control Mode.................. Disable
Multicast Storm Control Level................. 5 percent
Unicast Storm Control Mode.................... Disable
Unicast Storm Control Level................... 5 percent
```

Command example:

```
(NETGEAR Switch) #show storm-control 0/1

Bcast      Bcast        Mcast         Mcast        Ucast     Ucast
Intf       Mode         Level         Mode         Level     Mode      Level
------     ---------    ---------     ---------    --------  -------   --------
0/1        Disable      5% Disable    5% Disable   5%
```

Command example:

```
(NETGEAR Switch) #show storm-control all

Bcast      Bcast        Mcast         Mcast        Ucast     Ucast
Intf       Mode         Level         Mode         Level     Mode      Level
------     ---------    ---------     ---------    --------  -------   --------
0/1        Disable      5% Disable    5% Disable   5%
0/2        Disable      5% Disable    5% Disable   5%
```

```
0/3         Disable      5% Disable    5% Disable   5%
0/4         Disable      5% Disable    5% Disable   5%
0/5         Disable      5% Disable    5% Disable   5%
```

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

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

Use this command to display the status of LLPF rules configured on a particular port or on all ports..

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.

Term	Definition
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.

MRP Commands

Multicast Registration Protocol (MRP) replaces the Generic Attribute Registration Protocol (GARP) functionality. MRP provides the same functionality as GARP. MRP is a generic registration framework defined by the IEEE 802.1ak amendment to the IEEE 802.1Q standard.

Note: MRP commands are supported on M6100 series switches only.

mrp

This command sets the MRP protocol timers on an interface.

Format	`mrp {jointime` *`seconds`* `| leavetime` *`seconds`* `| leavealltime` *`seconds`*`}`
Mode	Interface Config

Parameter	Description
jointime *seconds*	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 factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is one centisecond (0.01 seconds).
leavetime *seconds*	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 6.0 seconds). The factory default is 300 centiseconds (3.0 seconds).
leavealltime *seconds*	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 factory default is 2000 centiseconds (20 seconds).

show mrp

This command displays MRP leave, join, and leaveall intervals configured on interfaces. If you specify the **summary** parameter, the output shows interval values for all interfaces. If you specify the *unit/slot/port* parameter, the output shows the MRP intervals for the specified interface.

Format	show mrp interface {summary | *unit/slot/port*}
Mode	Privileged Exec

MMRP Commands

mmrp (Global Config)

Use this command in Global Config mode to enable MMRP. MMRP must also be enabled on the individual interfaces.

Note: MMRP commands are supported on M6100 series switches only.

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

Use this command in Global Config mode to enable 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 MMRP periodic state machine.

Format	`no mmrp periodic state machine`
Mode	Global Config

mmrp (Interface Config)

Use this command in Interface Config mode on the interface. MMRP can be enabled on physical interfaces or 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	`mmrp`
Mode	Interface Config

no mmrp (Interface Config)

Use this command in Interface Config mode to disable MMRP mode on the interface.

Format	`no mmrp`
Mode	Global Config

clear mmrp statistics

Use this command in Privileged EXEC mode to clear MMRP statistics of one or all interfaces.

Format	`clear mmrp statistics [`*`unit/slot/port`*` | all]`
Mode	Privileged EXEC

Parameter	Description
unit/slot/port	If used with *`unit/slot/port`* parameter, the command clears MMRP statistics for the given interface.
all	If the **all** parameter is specified, the command clears MMRP statistics for all the interfaces.

show mmrp

Use this command in Privileged EXEC mode to display the status of the MMRP mode.

Format	`show mmrp [summary | interface [unit/slot/port | summary]]`
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 *unit/slot/port*, the command displays the MMRP mode of that interface.
summary	If **interface** is specified with the **summary** parameter, the command shows a table containing MMRP global mode 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
0/13      Disabled
0/14      Disabled
0/15      Disabled
```

```
0/16      Disabled
0/17      Disabled
```

show mmrp statistics

Use this command in Privileged EXEC mode to display statistical information about the MMRP PDUs sent and received on the interface.

Format	`show mmrp statistics {summary | [`*`unit/slot/port`*` | all]}`
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

MVRP Commands

mvrp (Global Config)

Use this command in Global Configuration mode to enable MVRP. MVRP must also be enabled on the individual interfaces.

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.

Note: MVRP commands are supported on M6100 series switches only.

Default	enabled
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

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)

Use this command in Interface Configuration mode to enable MVRP mode on the interface. The port should be configured in trunk or general mode. MVRP can be enabled on physical interfaces or LAG interfaces. When configured on a LAG member port, MVRP is operationally disabled. Enabling MVRP on an interface automatically enabled dynamic VLAN creation.

Default	enabled
Format	`mvrp`
Mode	Interface Config

no mvrp (Interface Config)

Use this command in Interface Configuration mode to disable MVRP mode on the interface.

Format	`no mvrp`
Mode	Interface Config

clear mvrp

Use this command in Privileged EXEC mode to clear the MVRP statistics of one or all interfaces.

Format	`clear mvrp statistics [`*`unit/slot/port`*` | all]`
Mode	Privileged EXEC

Parameter	Description
unit/slot/port	If used with the *`unit/slot/port`* parameter, the command clears MVRP statistics for the given interface.
all	If the **`all`** parameter is specified, the command clears MVRP statistics for all the interfaces.

show mvrp

Use this command in Privileged EXEC mode to display the status of the MVRP mode.

Format	`show mvrp [summary | interface [unit/slot/port | all]]`
Mode	Privileged EXEC

Parameter	Description
summary	If the **summary** parameter is used, the command shows global MVRP information.
interface	If the interface is specified as *unit/slot/port*, the command shows MVRP mode information for that interface.
all	If the interface is specified with the **all** parameter, the command shows a table containing MVRP global mode and the mode for all interfaces.

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
```

show mvrp statistics

Use this command in Privileged EXEC mode to display MVRP statistics.

Format	`show mvrp statistics [summary | unit/slot/port | all]`
Mode	Privileged EXEC

Parameter	Description
summary	If used with the **summary** parameter, the command shows global MVRP statistics.
interface	If the *unit/slot/port* is specified, the command shows MVRP statistics for that interface.
all	If used with the **all** parameter, the command shows a table containing MVRP statistics for all interfaces on which MVRP is enabled.

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
```

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 (LAG) interface 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

This command configures a new port-channel (LAG) and generates a logical *unit/slot/port* 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 *unit/slot/port* number for the logical 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.

Note: Before you include a port in a port-channel, set the port physical mode. For more information, see *speed* on page 360.

Format	`port-channel` *name*
Mode	Global Config

addport

This command adds one port to the port-channel (LAG). The first interface is a logical *unit/slot/port* 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**. 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.

Note: Before adding a port to a port-channel, set the physical mode of the port. For more information, see *speed* on page 360.

Format	`addport` *logical unit/slot/port*
Mode	Interface Config

deleteport (Interface Config)

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	`deleteport` *logical unit/slot/port*
Mode	Interface Config

deleteport (Global Config)

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	`deleteport {`*logical unit/slot/port* `| all}`
Mode	Global Config

lacp admin key

Use this command to configure the administrative value of the key for the port-channel. The value range of *key* is 0 to 65535.

Default	0x8000
Format	`lacp admin key` *key*
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

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 valid range of *delay* is 0-65535.

Default	0x8000
Format	`lacp collector max delay` *delay*
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

Use this command to configure the administrative value of the LACP actor admin key on an interface or range of interfaces. The valid range for *key* is 0-65535.

Default	Internal Interface Number of this Physical Port
Format	`lacp actor admin key` *key*
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 individual

Use this command to set LACP actor admin state to individual.

Format	`lacp actor admin state individual`
Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp actor admin state individual

Use this command to set the LACP actor admin state to aggregation.

Format	`no lacp actor admin state individual`
Mode	Interface Config

lacp actor admin state longtimeout

Use this command to set LACP actor admin state to longtimeout.

Format	`lacp actor admin state longtimeout`
Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp actor admin state longtimeout

Use this command to set the LACP actor admin state to short timeout.

Format	`no lacp actor admin state longtimeout`
Mode	Interface Config

Note: This command is applicable only to physical interfaces.

lacp actor admin state passive

Use this command to set the LACP actor admin state to passive.

Format	`lacp actor admin state passive`
Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp actor admin state passive

Use this command to set the LACP actor admin state to active.

Format	`no lacp actor admin state passive`
Mode	Interface Config

lacp actor admin state

Use this command to configure the administrative value of actor state as transmitted by the Actor in LACPDUs. This command can be used to configure a single interfaces 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 the configure the default administrative values of actor state as transmitted by the Actor 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

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	`lacp actor port priority` *`priority`*
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	`no lacp actor port priority`
Mode	Interface Config

lacp partner admin key

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	`lacp partner admin key` *key*
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

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

Use this command to set LACP partner admin state to longtimeout.

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 timeout.

Format	`no lacp partner admin state longtimeout`
Mode	Interface Config

Note: This command is applicable only to physical interfaces.

lacp partner admin state passive

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

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` *`port-id`*
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

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` *`priority`*
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

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` *`system-id`*
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

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` *`priority`*
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

Use this command to enter Interface configuration mode for the specified LAG.

Format	`interface lag` *`lag-interface-number`*
Mode	Global Config

port-channel static

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	enabled
Format	`port-channel static`
Mode	Interface 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	`no port-channel static`
Mode	Interface Config

port lacpmode

This command enables Link Aggregation Control Protocol (LACP) on a port or range of ports.

Default	enabled
Format	`port lacpmode`
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

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)

This command sets the timeout on a physical interface or range of interfaces of a particular device type (actor or partner) to either long or short timeout.

Default	long
Format	`port lacptimeout {actor | partner} {long | short}`
Mode	Interface Config

no port lacptimeout

This command sets the timeout back to its default value 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)

This command sets the timeout for all interfaces of a particular device type (actor or partner) to either long or short timeout.

Default	long
Format	`port lacptimeout {actor | partner} {long | short}`
Mode	Global Config

no port lacptimeout

This command sets the timeout for all physical interfaces of a particular device type (actor or partner) back to their default values.

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

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

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	enabled
Format	`port-channel linktrap {logical unit/slot/port | 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 {logical unit/slot/port | all}`
Mode	Global Config

port-channel load-balance

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}`
Mode	Interface 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

Term	Definition
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: **all** applies the command to all currently configured port-channels.

no port-channel load-balance

This command reverts to the default load balancing configuration.

Format	`no port-channel load-balance {`*`unit/slot/port`*` | all}`
Mode	Interface 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: **all** applies the command to all currently configured port-channels.

port-channel local-preference

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	disable
Format	`port-channel local-preference`
Mode	Interface 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 Config

port-channel min-links

This command configures the port-channel's minimum links for lag interfaces. The *number* parameter can be in the range 1–8. The default is 1.

Default	1

Format	`port-channel min-links` *`number`*
Mode	Interface Config

port-channel name

This command defines a name for the port-channel (LAG). The interface is a logical *`unit/slot/port`* for a configured port-channel, and *`name`* is an alphanumeric string up to 15 characters. 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	`port-channel name {`*`logical unit/slot/port`*`}` *`name`*
Mode	Global Config

port-channel system priority

Use this command to configure port-channel system priority. The valid range of *priority* is 0-65535.

Default	0x8000
Format	`port-channel system priority` *`priority`*
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

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 {`*`unit/slot/port`*` | 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.

Parameter	Description
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

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	`show lacp actor {`*unit/slot/port* `| all}`
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

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	`show port-channel brief`
Mode	User EXEC

For each port-channel the following information is displayed.

Term	Definition
Logical Interface	The *unit/slot/port* 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.

Term	Definition
Mbr Ports	The members of this port-channel.
Active Ports	The ports that are actively participating in the port-channel.

show port-channel

This command displays an overview of all port-channels (LAGs) on the switch.

Format	`show port-channel`
Mode	Privileged EXEC

Term	Definition
Logical Interface	The valid *`unit/slot/port`* number.
Port-Channel Name	The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.
Link State	Indicates whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Type	The status designating whether a particular port-channel (LAG) is statically or dynamically maintained. • Static. The port-channel is statically maintained. • Dynamic. The port-channel is dynamically maintained.
Load Balance Option	The load balance option associated with this LAG. See *port-channel load-balance* on page 489.
Local Preference Mode	Indicates whether the local preference mode is enabled or disabled.
Mbr Ports	A listing of the ports that are members of this port-channel (LAG), in *`unit/slot/port`* notation. There can be a maximum of eight ports assigned to a given port-channel (LAG).
Device Timeout	For each port, lists the timeout (long or short) for Device Type (actor or partner).
Port Speed	Speed of the port-channel port.
Active Ports	This field lists ports that are actively participating in the port-channel (LAG).

Command example:

```
(NETGEAR Switch) #show port-channel 0/3/1

Local Interface.............................. 0/3/1
Channel Name................................. ch1
Link State................................... Up
Admin Mode................................... Enabled
Type......................................... Static
```

```
Load Balance Option.......................... 3
(Src/Dest MAC, VLAN, EType, incoming port)
Local Preference Mode........................ Enabled

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
1/0/1  actor/long    Auto      True
       partner/long
1/0/2  actor/long    Auto      True
       partner/long
1/0/3  actor/long    Auto      False
       partner/long
1/0/4  actor/long    Auto      False
       partner/long
```

show port-channel system priority

Use this command to display the port-channel system priority.

Format	`show port-channel system priority`
Mode	Privileged EXEC

show port-channel counters

Use this command to display port-channel counters for the specified port.

Format	`show port-channel` *`unit/slot/port`* `counters`
Mode	Privileged EXEC

Term	Definition
Local Interface	The valid *`unit/slot/port`* number.
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 slot/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................................. ch1
Link State................................... Down
Admin Mode................................... Enabled
Port Channel Flap Count...................... 0

Mbr    Mbr Flap
Ports  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

Use this command to clear and reset specified port-channel and member flap counters for the specified interface.

Format	`clear port-channel {`*`lag-intf-num`* `|` *`unit/slot/port`*`} counters`
Mode	Privileged EXEC

clear port-channel all counters

Use this command to clear and reset all port-channel and member flap counters for the specified interface.

Format	`clear port-channel all counters`
Mode	Privileged EXEC

VPC Commands

VPC (also known as MLAG) enables a LAG to be created across two independent units, so that some member ports of a VPC can reside on one unit and the other members of a VPC can reside on another unit. The partner device on the remote side can be a VPC-unaware unit. To the unaware unit, the VPC appears to be a single LAG connected to a single unit.

Note: The VPC commands are supported only on the M6100 and M7100 series switches.

vpc domain

Use this command to enter into VPC configuration mode and create a VPC domain with the specified domain ID. You can create one VPC domain only on a device. The domain ID of the VPC domain must be the same as the one that is configured on the VPC peer with which the device must form a VPC pair. The configured VPC domain IDs are exchanged during role election. If the IDs are configured differently on the peer devices, the VPC does not become operational.

You must ensure that the no two VPC domains can share the same VPC domain ID. The domain ID is used to derive the autogenerated VPC MAC address that is used in the actor ID field in the LACP PDUs and STP BPDUs that are sent on VPC interfaces. If two VPC domains have the same domain ID, the information in the actor ID fields is identical, causing LACP convergence issues and STP convergence issues.

The range for *domain-id* is 1-255.

Format	`vpc domain` *domain-id*
Mode	Global Config

no vpc domain

Use this command to delete a VPC domain, disable peer keepalives, disable peer detection, and reset the configured parameters (the role priority, VPC MAC address, and VPC system priority) for the VPC domain.

Format	`no vpc domain` *domain-id*
Mode	Global Config

feature vpc

This command enables VPC globally. VPC role election occurs if both VPC and the keepalive state machine are enabled (see *peer-keepalive timeout* on page 499). Peer link also has to be configured for role election to occur.

Format	`feature vpc`
Mode	Global Config

no feature vpc

This command disables VPC.

Format	`no feature vpc`
Mode	Global Config

peer detection enable

This command starts the dual control plane detection protocol (DCPDP) on the VPC switch. The peer VPC switch's IP address must be configured for the DCPDP to start on an VPC switch.

Default	None
Format	`peer detection enable`
Mode	VPC Config

no peer detection enable

This command disables the dual control plane (DCPDP) detection protocol on the VPC switch.

Format	`no peer detection enable`
Mode	VPC Config

peer detection interval

Use this command to configure the DCPDP transmission interval and reception time-out.

The configurable transmission interval range is 200–4000 ms. The default transmission interval is 1000 ms.

The configurable reception time-out range is 700 ms–14 seconds. The default reception time-out is 3.5 seconds.

Default	Transmission interval: 1000 ms Reception time-out: 3.5 seconds
Format	`peer detection interval` *`msecs`* `timeout` *`msecs`*
Mode	VPC Config

no peer detection interval

Use this command to reset the DCPDP transmission interval and reception time-out to default values. The default transmission interval is 1000 ms. The default reception time-out is 3.5 seconds.

Format	`no peer detection interval` *`msecs`* `timeout` *`msecs`*
Mode	VPC Config

peer-keepalive destination

This command configures the IP address of the peer VPC switch, which is the destination IP address of the dual control plane detection protocol (DCPDP) on the peer VPC switch. This configuration is used by the dual control plane detection protocol (DCPDP) on the VPC switches. It also configures the source IP address of the DCPDP message, which is the self IP on the VPC switch. The UDP port on which the VPC switch listens to the DCPDP messages can also be configured with this command.

The configurable range for the UDP port 1 to 65535. The default is 60000.

Format	`peer-keepalive destination` *`ipaddress`* `source` *`ipaddress`* `[udp-port` *`port`*`]`
Mode	VPC Config

no peer-keepalive destination

This command unconfigures the self IP address, peer IP address, and the UDP port.

Format	`no peer-keepalive destination` *`ipaddress`* `source` *`ipaddress`*
Mode	VPC Config

peer-keepalive enable

This command starts the keepalive state machine on the VPC device, if VPC is globally enabled.

Default	`Disabled`
Format	`peer-keepalive enable`
Mode	VPC Config

no peer-keepalive enable

This command stops the keepalive state machine of the VPC switch.

Format	`no peer-keepalive enable`
Mode	VPC Config

peer-keepalive timeout

This command configures the peer keepalive timeout value (in seconds). If an VPC switch does not receive a keepalive message from the peer for the duration of this timeout value, it transitions its role (if required).

Note: The keepalive state machine is not restarted if keepalive priority is modified post election.

The configurable range is 2 to 15 seconds. The default is 5 seconds.

Default	5
Format	`peer-keepalive timeout` *`seconds`*
Mode	VPC Config

no peer-keepalive timeout

This command resets the keepalive timeout to the default value of 5 seconds.

Format	`no keepalive timeout`
Mode	VPC Config

role priority

This command configures VPC switch priority. This value is used for VPC role election. The priority value is sent to the peer in the VPC keepalive messages. The VPC switch with lower priority becomes the Primary and the switch with higher priority becomes the Secondary. If both VPC peer switches have the same role priority, the device with the lower system MAC address becomes the Primary.

Note: The keepalive state machine is not restarted even if the keepalive priority is modified post-election.

The priority can be between 1 and 255 seconds. The default is 100.

Default	`100`
Format	`role priority` *`seconds`*
Mode	VPC Config

no role priority

This command resets the keepalive priority and timeout to the default value of 100.

Format	`no role priority`
Mode	VPC Config

track vpc interface

This command enables shutting down local VPC members if a non-VPC link goes down. The local VPC members are brought up again if the link comes back up for the specified interface.

Default	`Disabled`
Format	`track vpc` *`vpc-id`* `interface` *`unit/slot/port`*
Mode	VPC Config

no track vpc interface

This command disables shutting down local VPC members if a non-VPC link goes down. The local VPC members are brought up again if the link comes back up for the specified interface.

Format	`no track vpc` *`vpc-id`* `interface` *`unit/slot/port`*
Mode	VPC Config

system-priority

Use this command to manually configure a system priority for the VPC domain. Configure the same system priority on both VPC peers. If the configured VPC system priority is different on the VPC peers, the VPC does not become operational.

If VPC primary device election occurs after you configure the VPC system priority, the configured priority value is used in the LACP PDUs and STP BPDUs that are sent on VPC member ports. If VPC primary device election occurs before you configure the VPC system priority, the operational VPC system priority value is used in the LACP PDUs and STP BPDUs instead of the configured VPC priority value.

The configurable priority range is from 1 to 65535.

Default	`32767`
Format	`system-priority` *`priority`*
Mode	VPC Config

no system-priority

This command restores the VPC system priority to the default value (32767).

Format	`no system-priority`
Mode	VPC Config

system-mac

Use this command to manually configure the MAC address for the VPC domain. Configure the VPC MAC address the same on both peer devices. The specified MAC address must be a unicast MAC address in the aa:bb:cc:dd:ee:ff format and cannot be equal to the MAC address of either the primary VPC or the secondary VPC device. The configured VPC MAC address is exchanged during role election. If the MAC addresses are configured differently on the peer devices, the VPC domain does not become operational.

If VPC primary device election occurs after you configure the VPC MAC address, the configured MAC address is used in the LACP PDUs and STP BPDUs that are sent on VPC member ports. If VPC primary device election occurs before you configure the VPC MAC address, the operational VPC MAC address is used in the LACP PDUs and STP BPDUs instead of the configured VPC MAC address.

By default, the VPC MAC address is automatically generated. For a NETGEAR switch, C0:FF:D4:A7:DA is used as the upper 40 bits in the automatically generated VPC MAC address. The lower 8 bits are derived from the VPC domain ID.

C0:FF:D4:A7:DA:<*VPC domain ID*>, in which <*VPC domain ID*> is the VPC domain ID, is the auto-generated VPC MAC address for a VPC domain ID. No two VPC domains in the network must be assigned the same domain ID. If two VPC domains in the network are assigned the same domain ID, the same VPC MAC addresses are autogenerated, causing LACP and STP convergence issues in the network.

The VPC MAC address range for NETGEAR switches is C0:FF:D4:A7:DA:00 to C0:FF:D4:A7:DA:FF.

Default	`C0:FF:D4:A7:DA:00 to C0:FF:D4:A7:DA:FF`
Format	`system-mac` *`mac-address`*
Mode	VPC Config

no system-mac

This command removes the manually configured VPC MAC address for the VPC domain.

Format	`no system-mac`
Mode	VPC Config

vpc

This command configures a port-channel (LAG) as part of an VPC. Upon issuing this command, the port-channel is down until the port-channel member information is exchanged and agreed between the VPC peer switches.

The configurable range for the VPC id 1 to the maximum number of LAG interfaces, which is 64 minus 1.

Default	none
Format	vpc *id*
Mode	LAG Interface

no vpc

This command unconfigures a port-channel as VPC.

Format	no vpc *id*
Mode	LAG Interface

vpc peer-link

This command configures a port channel as the VPC peer link.

Format	vpc peer-link
Mode	LAG Interface

no vpc peer-link

This command unconfigures a port channel as the VPC peer link.

Format	no vpc peer-link
Mode	LAG Interface

show vpc

This command displays information about an VPC. The configuration and operational modes of the VPC are displayed; the VPC is operationally enabled if all the preconditions are met. The port-channel that is configured as an VPC interface is also displayed with the member ports on the current switch and peer switch (with their link status).

Format	show vpc *id*
Mode	User EXEC

Command example:

```
(NETGEAR Switch) # show vpc 10
VPC id#10
-----------------
Config mode.....................................Enabled
Operational mode...............................Enabled
Port channel.....................................3/1
Self member ports Status
----------------- ---------
              0/2 UP
              0/6 DOWN
Peer member ports Status
----------------- ---------
              0/8 UP
```

show vpc brief

This command displays the VPC global status and current VPC operational mode (the VPC is in operational mode if the preconditions are met). The peerlink and keepalive statuses as well as the number of configured and operational VPCs and the system MAC and role are displayed.

Format	show vpc brief
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) # show vpc brief
VPC config Mode.............................. Enabled
Keepalive config mode........................ Enabled
VPC operational Mode......................... Enabled
Self Role.................................... Primary
Peer Role.................................... Secondary
Peer detection............................... Disabled

Peer-Link details
-----------------
Interface.................................... 3/2
Peer link status............................. UP
Peer-link STP Mode........................... Disabled
Configured Vlans............................. 1
Egress tagging............................... none

VPC Details
-----------
Number of VPCs configured.................... 1
```

```
Number of VPCs operational..................... 1

VPC id# 1
-----------
Interface...................................... 3/1
Configured Vlans............................... 1
VPC Interface State............................ Active

Local MemberPorts       Status
-----------------       ------
             0/19       UP
             0/20       UP
             0/21       UP
             0/22       UP

Peer MemberPorts        Status
----------------        ------
            0/27        UP
            0/28        UP
            0/29        UP
            0/30        UP
```

show vpc peer-keepalive

This command displays the peer VPC switch IP address used by the dual control plane detection protocol. The port used for the DCPDP is shown. This command also displays if peer detection is enabled. If enabled, the detection status is displayed.

Format	`show vpc peer-keepalive`
Mode	User EXEC

Command example:

```
(NETGEAR Switch) # show vpc peer-keepalive
Peer IP address ……..... 10.130.14.55
Source IP address……..... 10.130.14.54
UDP port …….……..... 60000
Peer detection ……..…..... ENABLED
Peer is detected…….…..... TRUE
```

show vpc role

This command displays information about the keepalive status and parameters. The role of the VPC switch as well as the system MAC address and priority are displayed.

Format	`show vpc role`
Mode	User EXEC

Command example:

```
(NETGEAR Switch) # show vpc role
Self
----
Keepalive config mode..... Enabled
Keepalive operational mode..... Enabled
Priority..... 100
System MAC..... 00:10:18:82:18:63
Timeout..... 5
VPC State..... Primary
VPC Role..... Primary

Peer
----
Priority..... 100
VPC Role..... Secondary
System MAC..... 00:10:18:82:1b:ab
```

show vpc statistics

This command displays counters for the keepalive messages transmitted and received by the VPC switch.

Format	`show vpc statistics {peer-keepalive | peer-link}`
Mode	User EXEC

Command example:

```
(NETGEAR Switch) # show vpc statistics peer-keepalive
Total trasmitted..... 123
Tx successful..... 118
Tx errors..... 5
Total received..... 115
Rx successful..... 108
Rx Errors..... 7
Timeout counter..... 6
```

Command example:

```
(NETGEAR Switch) #show vpc statistics peer-link
Peer link control messages trasmitted…….... 123
Peer link control messages Tx errors.......... 5
Peer link control messages Tx timeout…….…….. 4
Peer link control messages ACK transmitted……. 34
Peer link control messages ACK Tx erorrs……. 5
Peer link control messages received..……. 115
Peer link data messages trasmitted……. 123
Peer link data messages Tx errors.............. 5
Peer link data messages Tx imeout…….……... 4
Peer link data messages ACK transmitted……. 34
Peer link data messages ACK Tx erorrs……. 5
Peer link data messages received….....……. 115
Peer link BPDU’s tranmsitted to peer……. 123
Peer link BPDU’s Tx error…….. 9
Peer link BPDU’s received from peer……. 143
Peer link BPDU’s Rx error…….. 1
Peer link LACPDU’s tranmsitted to peer……. 123
Peer link LACPDU’s Tx error…….. 9
Peer link LACPDU’s received from peer……. 143
Peer link LACPDU’s Rx error…….. 1
```

show vpc consistency-parameters

This command displays global consistency parameters and LAG interface consistency parameters for virtual port channels (VPC) on an MLAG switch.

Format	`show vpc consistency-parameters {global | interface lag` *`lag-intf-num`*`}`
Mode	Privileged Exec

Command example:

```
(NETGEAR Switch) #show vpc consistency-parameters global

Parameter                     Value
------------------------      ------------------------------------------------
STP Mode                      Enabled
STP Version                   IEEE 802.1w
BPDU Filter Mode              Disabled
BPDU Guard Mode               Disabled
No MST instances to display.
FDB Age Time                  300 seconds

MST VLAN Configuration
```

```
Instance        Associated VLANS
----------     ------------------------------------------------
01, 10
```

Command example:

```
(NETGEAR Switch) #show vpc consistency-parameters interface lag 2

Parameter                    Value
-------------------------    ---------------------------------------------
Port Channel Mode            Enabled
STP Mode                     Enabled
BPDU Filter Mode             Disabled
BPDU Flood Mode              Disabled
Auto-edge                    True
TCN Guard                    False
Port Cost                    0
Edge Port                    False
Root Guard                   False
Loop Guard                   False
Hash Mode                    3
Minimum Links                1
Channel Type                 Dynamic
Configured VLANs             1,10
MTU                          1518

Active Port     Speed       Duplex
------------    ---------   --------
1/0/23          1000        Full
```

clear vpc statistics

This command clears all the keepalive statistics.

Format	`clear vpc statistics {peer-keepalive | peer-link}`
Mode	User EXEC

Command example:

```
(NETGEAR Switch) # clear vpc statistics peer-keepalive
(NETGEAR Switch) # clear vpc statistics peer-link
```

debug vpc core

This command enables debug traces for VPC core functionality.

Note: To display the debug trace, enable the *debug console* command.

Format	`debug vpc core`
Mode	Privileged EXEC

debug vpc peer-keepalive

This command enables debug traces of the keepalive state machine transitions.

Note: To display the debug trace, enable the *debug console* command.

Format	`debug vpc peer-keepalive`
Mode	User EXEC

debug vpc peer-link data-message

This command enables debug traces for control messages that are exchanged between the VPC devices on the peer link.

Format	`debug vpc peer-link data-message`
Mode	User EXEC

debug vpc peer-link control-message async

This command enables debug traces for asynchronous reliable control messages that are exchanged between MLAG devices on the peer link. For errors, only the errors in the communication are traced. For messages, the control message contents that are exchanged can be traced. Both transmitted and received control messages contents can be traced.

Format	`debug vpc peer-link control-message async {error | msg [receive | transmit]}`
Mode	User EXEC

debug vpc peer-link control-message bulk

This command enables debug traces for periodic control messages that are exchanged between MLAG devices on the peer link. For errors, only the errors in the communication are traced. For messages, the control message contents that are exchanged can be traced. Both transmitted and received control messages contents can be traced.

Format	`debug vpc peer-link control-message bulk {error | msg [receive | transmit]}`
Mode	User EXEC

debug vpc peer-link control-message ckpt

This command enables debug traces for checkpointing control messages that are exchanged between MLAG devices on the peer link. For errors, only the errors in the communication are traced. For messages, the control message contents that are exchanged can be traced. Both transmitted and received control messages contents can be traced.

Format	`debug vpc peer-link control-message ckpt {error | msg [receive | transmit]}`
Mode	User EXEC

debug vpc peer detection

This command enables debug traces for the dual control plane detection protocol. Traces are seen when the DCPDP transmits or receives detection packets to or from the peer VPC switch.

Note: To display the debug trace, enable the *debug console* command.

Format	`debug vpc peer detection`
Mode	User 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

This command configures a probe port and a monitored port for monitor session (port monitoring). Use the **`source interface`** *`unit/slot/port`* parameter to specify the interface to monitor. 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.

A VLAN can be configured as the source to a session (all member ports of that VLAN are monitored). Remote port mirroring is configured by adding the RSPAN VLAN ID. At the source switch, the destination is configured as the RSPAN VLAN and at the destination switch, the source is configured as the RSPAN VLAN.

Note: The source and destination cannot be configured as remote on the same device.

The reflector-port is configured at the source switch. The reflector-port forwards the mirrored traffic towards the destination switch.

Note: This port must be configured with RSPAN VLAN membership.

IP/MAC ACL can be attached to a session by giving the access list number/name.

Use the **destination interface** *unit/slot/port* to specify the interface to receive the monitored traffic.

Use the **mode** parameter to enable the administrative mode of the session. If enabled, the probe port monitors all the traffic received and transmitted on the physical monitored port.

Use the filter parameter to filter a specified access group either by IP address or MAC address.

Format	monitor session *session-id* {source {interface *unit/slot/port* | cpu || vlan *vlan-id* | remote vlan *vlan-id* }[{rx | tx}] | destination {interface *unit/slot/port* |remote vlan *vlan-id* reflector-port *unit/slot/port*}| mode | filter {ip access-group [*acl-id* | *aclname*] |mac access-group *acl-name*}}
Mode	Global Config

Command example:

To configure the RSPAN VLAN source:

```
monitor session session-id source {interface unit/slot/port | vlan vlan-id | remote vlan
vlan-id }[rx | tx]
```

Command example:

To the configure RSPAN VLAN destination:

```
monitor session session-id destination {interface unit/slot/port | remote vlan vlan-id
reflector-port unit/slot/port}
```

Command example:

To attach an ACL:

```
monitor session session-id filter {ip access-group [acl-id | aclname] | mac access-group
acl-name}
```

no monitor session

Use this command without optional parameters to remove the monitor session (port monitoring) designation from the source probe port, the destination monitored port and all VLANs. Once the port is removed from the VLAN, you must manually add the port to any desired VLANs. Use the **source interface** *unit/slot/port* parameter or **destination interface** to remove the specified interface from the port monitoring session. Use the **mode** parameter to disable the administrative mode of the session.

Note: Because the current version of NETGEAR Managed Switch software only supports one session, if you do not supply optional parameters, the behavior of this command is similar to the behavior of the **no monitor** command.

Format	`no monitor session` *`session-id`* `[{source interface` *`unit/slot/port`* `| destination interface | mode |filter {ip access-group |mac access-group}}]`
Mode	Global Config

no monitor

This command removes all the source ports and a destination port for the and restores the default value for mirroring session mode for all the configured sessions.

Note: This is a stand-alone no command. This command does not have a normal form.

Default	enabled
Format	`no monitor`
Mode	Global Config

show monitor session

This command displays the port monitoring information for a particular mirroring session.

Note: 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 always one (1).

Format	`show monitor session` *`session-id`*
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 *`session-id`*. The possible values are Enabled and Disabled.

Term	Definition
Probe Port	Probe port (destination port) for the session identified with *session-id*. 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 *session-id*. 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

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
```

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

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	`macfilter` *`macaddr vlanid`*
Mode	Global Config

no macfilter

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	`no macfilter` *`macaddr vlanid`*
Mode	Global Config

macfilter adddest

Use this command to add the interface or range of interfaces to the destination filter set for the MAC filter with the given *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	`macfilter adddest` *`macaddr vlanid`*
Mode	Interface Config

no macfilter adddest

This command removes a port from the destination filter set for the MAC filter with the given *`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	`no macfilter adddest` *`macaddr vlanid`*
Mode	Interface Config

macfilter adddest all

This command adds all interfaces to the destination filter set for the MAC filter with the given *`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	`macfilter adddest all` *`macaddr vlanid`*
Mode	Global Config

no macfilter adddest all

This command removes all ports from the destination filter set for the MAC filter with the given *`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	`no macfilter adddest all` *`macaddr vlanid`*
Mode	Global Config

macfilter addsrc

This command adds the interface or range of interfaces to the source filter set for the MAC filter with the MAC filter with the given *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	`macfilter addsrc` *macaddr vlanid*
Mode	Interface Config

no macfilter addsrc

This command removes a port from the source filter set for the MAC filter with the given *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	`no macfilter addsrc` *macaddr vlanid*
Mode	Interface Config

macfilter addsrc all

This command adds all interfaces to the source filter set for the MAC filter with the MAC filter with the given *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	`macfilter addsrc all` *macaddr vlanid*
Mode	Global Config

no macfilter addsrc all

This command removes all interfaces to the source filter set for the MAC filter with the given *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	`no macfilter addsrc all` *macaddr vlanid*
Mode	Global Config

show mac-address-table static

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	`show mac-address-table static {`*`macaddr vlanid`*` | all}`
Mode	Privileged EXEC

Term	Definition
MAC Address	The MAC Address of the static MAC filter entry.
VLAN ID	The VLAN ID of the static MAC filter entry.
Source Ports	The source port filter set slot and ports.

Note: Only multicast address filters can have destination port lists.

show mac-address-table staticfiltering

This command displays the Static Filtering entries in the Multicast Forwarding Database (MFDB) table.

Format	`show mac-address-table staticfiltering`
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

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	`dhcp l2relay`
Mode	Global Config Interface Config

no dhcp l2relay

This command disables DHCP Layer 2 relay agent for an interface or range of interfaces.

Format	`no dhcp l2relay`
Mode	Global Config Interface Config

dhcp l2relay circuit-id vlan

This parameter sets the DHCP Option-82 Circuit ID for a VLAN. When enabled, the interface number is added as the Circuit ID in DHCP option 82.

Format	`dhcp l2relay circuit-id vlan` *`vlan-list`*
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 circuit-id vlan

This parameter clears the DHCP Option-82 Circuit ID for a VLAN.

Format	`no dhcp l2relay circuit-id vlan` *`vlan-list`*
Mode	Global Config

dhcp l2relay remote-id subscription

This command sets the Option-82 Remote-ID string for a given service subscription identified by *`subscription-string`* on a given interface or range of interfaces. The *subscription-string* is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. The *`remoteid-string`* is a character string. When remote-id string is set using this command, all Client DHCP requests that fall

under this service subscription are added with Option-82 Remote-id as the configured remote-id string.

Default	empty string
Format	`dhcp l2relay remote-id` *`remoteid-string`* `subscription-name` *`subscription-string`*
Mode	Interface Config

no dhcp l2relay remote-id subscription

This command resets the Option-82 Remote-ID string for a given service subscription identified by *`subscription-string`* on a given interface. The *`subscription-string`* is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When remote-id string is reset using this command, the Client DHCP requests that fall under this service subscription are not added with Option-82 Remote-id.

Format	`no dhcp l2relay remote-id` *`remoteid-string`* `subscription-name` *`subscription-string`*
Mode	Interface Config

dhcp l2relay remote-id vlan

This parameter sets the DHCP Option-82 Remote ID for a VLAN and subscribed service (based on subscription-name).

Format	`dhcp l2relay remote-id` *`remote-id-string`* `vlan` *`vlan-list`*
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 and subscribed service (based on subscription-name).

Format	`no dhcp l2relay remote-id vlan` *`vlan-list`*
Mode	Global Config

dhcp l2relay subscription

This command enables relaying DHCP packets on an interface or range of interfaces that fall under the specified service subscription. The *subscription-string* is a character string that must be matched with the configured DOT1AD subscription-string for correct operation.

Default	disabled (that is, no DHCP packets are relayed)
Format	`dhcp l2relay subscription-name` *`subscription-string`*
Mode	Interface Config

no dhcp l2relay subscription

This command disables relaying DHCP packets that fall under the specified service subscription. The *subscription-string* is a character string that must be matched with the configured DOT1AD subscription string for correct operation.

Format	`no dhcp l2relay subscription-name` *`subscription-string`*
Mode	Interface Config

dhcp l2relay trust

Use this command to configure an interface or range of interfaces as trusted for Option-82 reception.

Default	untrusted
Format	`dhcp l2relay trust`
Mode	Interface Config

no dhcp l2relay trust

Use this command to configure an interface to the default untrusted for Option-82 reception.

Format	`no dhcp l2relay trust`
Mode	Interface Config

dhcp l2relay vlan

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	disable
Format	`dhcp l2relay vlan` *`vlan-list`*
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` *`vlan-list`*
Mode	Global Config

show dhcp l2relay all

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

This command displays DHCP circuit-id vlan configuration.

Format	`show dhcp l2relay circuit-id vlan` *`vlan-list`*
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

This command displays DHCP L2 relay configuration specific to interfaces.

Format	`show dhcp l2relay interface {all | unit/slot/port}`
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

This command displays DHCP Remote-id vlan configuration.

Format	`show dhcp l2relay remote-id vlan vlan-list`
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

This command displays statistics specific to DHCP L2 Relay configured interface.

Format	`show dhcp l2relay stats interface {all | unit/slot/port}`
Mode	Privileged EXEC

Command example:

```
((NETGEAR Switch)) #show dhcp l2relay stats interface all

DHCP L2 Relay is  Enabled.

Interface  UntrustedServer    UntrustedClient  TrustedServer     TrustedClient
           MsgsWithOpt82      MsgsWithOpt82    MsgsWithoutOpt82  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 subscription interface

This command displays DHCP L2 Relay configuration specific to a service subscription on an interface.

Format	`show dhcp l2relay subscription interface {all | unit/slot/port}`
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show dhcp l2relay subscription interface all
Interface    SubscriptionName    L2Relay mode  Circuit-Id mode  Remote-Id mode
-----------  ----------------   -------------- ---------------  ----------------
  0/1             sub1             Enabled       Disabled         --NULL--
  0/2             sub3             Enabled       Disabled         EnterpriseSwitch
  0/2             sub22            Disabled      Enabled          --NULL--
  0/4             sub4             Enabled       Enabled          --NULL--
```

show dhcp l2relay agent-option vlan

This command displays the DHCP L2 Relay Option-82 configuration specific to VLAN.

Format	`show dhcp l2relay agent-option vlan vlan-range`
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

This command displays DHCP vlan configuration.

Format	`show dhcp l2relay vlan` *`vlan-list`*
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

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.

Format	`clear dhcp l2relay statistics interface {`*`unit/slot/port`* `| all}`
Mode	Privileged EXEC

DHCP Client Commands

NETGEAR Managed 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

This command enables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the NETGEAR Managed Switch switch.

Format	`dhcp client vendor-id-option` *`string`*
Mode	Global Config

no dhcp client vendor-id-option

This command disables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the NETGEAR Managed Switch switch.

Format	`no dhcp client vendor-id-option`
Mode	Global Config

dhcp client vendor-id-option-string

This parameter sets the DHCP Vendor Option-60 string to be included in the requests transmitted to the DHCP server by the DHCP client operating in the NETGEAR Managed Switch switch.

Format	`dhcp client vendor-id-option-string` *`string`*
Mode	Global Config

no dhcp client vendor-id-option-string

This parameter clears the DHCP Vendor Option-60 string.

Format	`no dhcp client vendor-id-option-string`
Mode	Global Config

show dhcp client vendor-id-option

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

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

Use this command to enable DHCP Snooping on a list of comma-separated VLAN ranges.

Default	disabled
Format	`ip dhcp snooping vlan` *`vlan-list`*
Mode	Global Config

no ip dhcp snooping vlan

Use this command to disable DHCP Snooping on VLANs.

Format	`no ip dhcp snooping vlan` *`vlan-list`*
Mode	Global Config

ip dhcp snooping verify mac-address

Use this command to enable verification of the source MAC address with the client hardware address in the received DCHP message.

Default	enabled
Format	`ip dhcp snooping verify mac-address`
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	`no ip dhcp snooping verify mac-address`
Mode	Global Config

ip dhcp snooping database

Use this command to configure the persistent location of the DHCP Snooping database. This can be local or a remote file on a given IP machine.

Default	local
Format	`ip dhcp snooping database {local | tftp://`*`hostIP/filename`*`}`
Mode	Global Config

ip dhcp snooping database write-delay (DHCP)

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	`ip dhcp snooping database write-delay` *`seconds`*
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

ip dhcp snooping binding

Use this command to configure static DHCP Snooping binding.

Format	`ip dhcp snooping binding` *`mac-address`* `vlan` *`vlan-id ipaddress`* `interface` *`interface-id`*
Mode	Global Config

no ip dhcp snooping binding

Use this command to remove the DHCP static entry from the DHCP Snooping database.

Format	`no ip dhcp snooping binding` *`mac-address`*
Mode	Global Config

ip verify binding

Use this command to configure static IP source guard (IPSG) entries.

Format	`ip verify binding` *`mac-address`* `vlan` *`vlan-id ipaddress`* `interface` *`interface-id`*
Mode	Global Config

no ip verify binding

Use this command to remove the IPSG static entry from the IPSG database.

Format	`no ip verify binding` *`mac-address`* `vlan` *`vlan-id ipaddress`* `interface` *`interface-id`*
Mode	Global Config

ip dhcp snooping limit

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.

Default	disabled (no limit)
Format	`ip dhcp snooping limit {rate` *`pps`* `[burst interval` *`seconds`*`]}`
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	`no ip dhcp snooping limit`
Mode	Interface Config

ip dhcp snooping log-invalid

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	`ip dhcp snooping log-invalid`
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	`no ip dhcp snooping log-invalid`
Mode	Interface Config

ip dhcp snooping trust

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

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

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

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 DCHP snooping.
- **`interface`** *`unit/slot/port`*. Restrict the output based on a specific interface.
- *`vlan-id`*. Restrict the output based on a VLAN.

Format	`show ip dhcp snooping binding [static | dynamic] [interface` *`unit/slot/port`*`] [`*`vlan-id`*`]`
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

Use this command to display the DHCP Snooping configuration related to the database persistency.

Format	`show ip 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 ip dhcp snooping database

agent url:  /10.131.13.79:/sai1.txt

write-delay:  5000
```

show ip dhcp snooping interfaces

Use this command to show the DHCP Snooping status of the interfaces.

Format	`show ip dhcp snooping interfaces`
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show ip dhcp snooping interfaces

 Interface    Trust State  Rate Limit   Burst Interval
                              (pps)       (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   Burst Interval
                              (pps)       (seconds)
-----------   ----------   ----------   --------------
```

```
1/0/15            Yes            15            1
```

show ip dhcp snooping statistics

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   Client Ifc   DHCP Server
               Failures     Mismatch    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

Use this command to clear all DHCP Snooping bindings on all interfaces or on a specific interface.

Format	`clear ip dhcp snooping binding [interface` *`unit/slot/port`*`]`
Mode	Privileged EXEC User EXEC

clear ip dhcp snooping statistics

Use this command to clear all DHCP Snooping statistics.

Format	`clear ip dhcp snooping statistics`
Mode	Privileged EXEC User EXEC

show ip verify source

Use this command to display the IPSG configurations on all ports.

Format	`show ip verify source`
Mode	Privileged EXEC User EXEC

Term	Definition
Interface	Interface address in *`unit/slot/port`* format.
Filter Type	Is 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 verify interface

Use this command to display the IPSG filter type for a specific interface.

Format	`show ip verify interface` *`unit/slot/port`*
Mode	Privileged EXEC User EXEC

Term	Definition
Interface	Interface address in *`unit/slot/port`* format.
Filter Type	Is 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 source binding

Use this command to display the IPSG bindings.

Format	`show ip source binding [dhcp-snooping | static] [interface` *`unit/slot/port`*`]` `[`*`vlan-id`*`]`
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 *`unit/slot/port`* 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

Use this command to enable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Default	`disabled`
Format	`ip arp inspection vlan` *`vlan-list`*
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	`no ip arp inspection vlan` *`vlan-list`*
Mode	Global Config

ip arp inspection validate

Use this command to enable additional validation checks like source-mac (src-mac) validation, destination-mac (dst-mac) validation, and IP address validation on the received ARP packets. Each 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	`ip arp inspection validate {[src-mac] [dst-mac] [ip]}`
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]}`
Mode	Global Config

ip arp inspection vlan logging

Use this command to enable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Default	`enabled`
Format	`ip arp inspection vlan` *`vlan-list`* `logging`
Mode	Global Config

no ip arp inspection vlan logging

Use this command to disable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Format	`no ip arp inspection vlan` *`vlan-list`* `logging`
Mode	Global Config

ip arp inspection trust

Use this command to configure an interface or range of interfaces as trusted for Dynamic ARP Inspection.

Default	`enabled`
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

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 pps value shown in the range for the rate option might be more than the hardware allowable limit. Therefore you need to understand the switch performance and configure the maximum rate pps accordingly.

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

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 given, 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	`ip arp inspection filter` *`acl-name`* `vlan` *`vlan-list`* `[static]`
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	`no ip arp inspection filter` *`acl-name`* `vlan` *`vlan-list`* `[static]`
Mode	Global Config

arp access-list

Use this command to create an ARP ACL.

Format	`arp access-list` *`acl-name`*
Mode	Global Config

no arp access-list

Use this command to delete a configured ARP ACL.

Format	`no arp access-list` *`acl-name`*
Mode	Global Config

permit ip host mac host

Use this command to configure a rule for a valid IP address and MAC address combination used in ARP packet validation.

Format	`permit ip host` *`sender-ipaddress`* `mac host` *`sender-mac`*
Mode	ARP Access-list Config

no permit ip host mac host

Use this command to delete a rule for a valid IP and MAC combination.

Format	`no permit ip host` *`sender-ipaddress`* `mac host` *`sender-mac`*
Mode	ARP Access-list Config

show ip arp inspection

Use this command to display the Dynamic ARP Inspection global configuration and configuration on all the VLANs. With the **`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 given 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	`show ip arp inspection [vlan` *`vlan-list`*`]`
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.
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

Use this command to display the statistics of the ARP packets that are processed by Dynamic ARP Inspection (DAI). 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. 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.
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

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

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. Given a *unit/slot/port* interface argument, the command displays the values for that interface whether the interface is enabled for DAI or not.

Format	`show ip arp inspection interfaces [`*`unit/slot/port`*`]`
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   Burst Interval
                                    (pps)        (seconds)
 ---------------  -----------   ----------  ---------------
 0/1                Untrusted           15                1
 0/2                Untrusted           10               10
```

show arp access-list

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 [`*`acl-name`*`]`
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
```

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.

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

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

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	`mvr group` *`A.B.C.D`* `[count]`
Mode	Global Config

no mvr group

This command removes the MVR membership group.

Format	`no mvr group A.B.C.D [count]`
Mode	Global Config

mvr mode

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	`mvr mode {compatible | dynamic}`
Mode	Global Config

no mvr mode

This command sets the mode type to the default value.

Format	`no mvr mode`
Mode	Global Config

mvr querytime

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	`mvr querytime deciseconds`
Mode	Global Config

no mvr querytime

This command sets the MVR query response time to the default value.

Format	`no mvr querytime`
Mode	Global Config

mvr vlan

This command sets the MVR multicast VLAN.

Default	1
Format	`mvr vlan` *`vlan-id`*
Mode	Global Config

no mvr vlan

This command sets the MVR multicast VLAN to the default value.

Format	`no mvr vlan`
Mode	Global Config

mvr immediate

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	`mvr immediate`
Mode	Interface Config

no mvr immediate

This command sets the MVR multicast VLAN to the default value.

Format	`no mvr immediate`
Mode	Interface Config

mvr type

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	`mvr type {receiver | source}`
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

Use this command to include the port in the specific MVR group. *mVLAN* is the multicast VLAN, and *A.B.C.D* is the IP multicast group.

Format	`mvr vlan` *mVLAN* `group` *A.B.C.D*
Mode	Interface Config

no mvr vlan

Use this command to exclude the port from the specific MVR group.

Format	`no mvr vlan` *mVLAN* `group` *A.B.C.D*
Mode	Interface Config

show mvr

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.
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

This command displays the MVR membership groups allocated. *A.B.C.D* is a valid multicast address in IPv4 dotted notation.

Format	`show mvr members [A.B.C.D]`
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

This command displays the MVR-enabled interfaces configuration.

Format	`show mvr interface [interface-id [members [vlan vid]]]`
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

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
```

IGMP Snooping Configuration Commands

This section describes the commands you use to configure IGMP snooping. NETGEAR Managed Switch software 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

This command enables IGMP Snooping on the system (Global Config Mode), an interface, or a range of interfaces. This command also enables IGMP snooping on a particular VLAN (VLAN Config 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.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

Default	disabled
Format	`set igmp [vlan-id]`
Mode	Global Config Interface Config VLAN Config

no set igmp

This command disables IGMP Snooping on the system, an interface, a range of interfaces, or a VLAN.

Format	`no set igmp [vlan-id]`
Mode	Global Config Interface Config VLAN Config

set igmp interfacemode

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.

Format	`no set igmp interfacemode`
Mode	Global Config

set igmp fast-leave

This command enables or disables IGMP Snooping fast-leave admin mode on a selected interface, a range of interfaces, or a VLAN. Enabling fast-leave allows the switch to immediately remove the layer 2 LAN interface from its forwarding table entry upon receiving

an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface.

You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP version 2 hosts.

Default	disabled
Format	`set igmp fast-leave [vlan-id]`
Mode	Interface Config Interface Range VLAN Config

no set igmp fast-leave

This command disables IGMP Snooping fast-leave admin mode on a selected interface.

Format	`no set igmp fast-leave [vlan-id]`
Mode	Interface Config Interface Range VLAN Config

set igmp groupmembership-interval

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	`set igmp groupmembership-interval [vlan-id] seconds`
Mode	Interface Config Global Config VLAN Config

no set igmp groupmembership-interval

This command sets the IGMPv3 group membership interval time to the default value.

Format	`no set igmp groupmembership-interval [vlan-id]`
Mode	Interface Config Global Config VLAN Config

set igmp maxresponse

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 25 seconds.

Default	10 seconds
Format	`set igmp maxresponse [vlan-id] seconds`
Mode	Global Config Interface Config VLAN Config

no set igmp maxresponse

This command sets the max response time (on the interface or VLAN) to the default value.

Format	`no set igmp maxresponse [vlan-id]`
Mode	Global Config Interface Config VLAN Config

set igmp mcrtrexpiretime

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	`set igmp mcrtrexpiretime [vlan-id] seconds`
Mode	Global Config Interface Config VLAN Config

no set igmp mcrtrexpiretime

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	`no set igmp mcrtrexpiretime [vlan-id]`
Mode	Global Config Interface Config VLAN Config

set igmp mrouter

This command configures the VLAN ID that has the multicast router mode enabled.

Format	`set igmp mrouter vlan-id`
Mode	Interface Config

no set igmp mrouter

This command disables multicast router mode for a particular VLAN ID.

Format	`no set igmp mrouter vlan-id`
Mode	Interface Config

set igmp mrouter interface

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	`set igmp mrouter interface`
Mode	Interface Config

no set igmp mrouter interface

This command disables the status of the interface as a statically configured multicast router interface.

Format	`no set igmp mrouter interface`
Mode	Interface Config

set igmp report-suppression

Use this command to suppress the IGMP reports on a given VLAN ID. In order 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 MGMD 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	`set igmp report-suppression` *`vlan-id`*
Mode	VLAN Config

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

set igmp header-validation

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 disabled the IGMP IP header validation.

Format	`no set igmp header-validation`
Mode	Global Config

show igmpsnooping

This command displays IGMP Snooping information for a given *`unit/slot/port`* or VLAN. Configured information is displayed whether or not IGMP Snooping is enabled.

Format	`show igmpsnooping [`*`unit/slot/port`* `|` *`vlan-id`*`]`
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 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, 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	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	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	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.

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.
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 554) in enabled or not.

Command example:

```
(NETGEAR switch) #show igmpsnooping 1

VLAN ID..................................... 1
IGMP Snooping Admin Mode.................... Disabled
Fast Leave Mode............................. Disabled
Group Membership Interval (secs)............ 260
Max Response Time (secs).................... 10
Multicast Router Expiry Time (secs)......... 0
Report Suppression Mode..................... Enabled
```

show igmpsnooping mrouter interface

This command displays information about statically configured ports.

Format	`show igmpsnooping mrouter interface` *unit/slot/port*
Mode	Privileged EXEC

Term	Definition
Interface	The port on which multicast router information is being displayed.

Term	Definition
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

This command displays information about statically configured ports.

Format	`show igmpsnooping mrouter vlan` *`unit/slot/port`*
Mode	Privileged EXEC

Term	Definition
Interface	The port on which multicast router information is being displayed.
VLAN ID	The list of VLANs of which the interface is a member.

show igmpsnooping ssm

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	`show igmpsnooping ssm {entries | groups | stats}`
Mode	Privileged EXEC

show mac-address-table igmpsnooping

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 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 querier

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	disabled
Format	`set igmp querier [`*`vlan-id`*`] [address `*`ipaddress`*`]`
Mode	Global Config 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 [vlan-id] [address]`
Mode	Global Config VLAN Mode

set igmp querier query-interval

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	disabled
Format	`set igmp querier query-interval seconds`
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

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 seconds`
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

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}`
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

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`
Mode	VLAN Config

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`
Mode	VLAN Config

show igmpsnooping querier

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.
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

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, on a particular VLAN and all interfaces participating in the VLAN.

By default, the proxy querrier is enabled.

Default	enabled
Format	`set igmp proxy-querier [vlan-id]`
Mode	Global Config Interface Config VLAN Config

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, on a particular VLAN and all interfaces participating in the VLAN.

This command is specific to IGMP.

Format	`no set igmp proxy-querier [vlan-id]`
Mode	Global Config Interface Config VLAN Config

show igmpsnooping proxy-querier

This command shows the global admin mode of the IGMP snooping proxy-querier and the interface on which it is enabled.

Format	`show igmpsnooping proxy-querier`
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 system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

set mld

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.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

Default	disabled
Format	`set mld vlan-id`
Mode	Global Config Interface Config VLAN Mode

no set mld

Use this command to disable MLD Snooping on the system.

Format	`no set mld vlan-id`
Mode	Global Config Interface Config VLAN Mode

set mld interfacemode

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

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: You should enable fast-leave admin mode only on VLANs where only one host is connected to each Layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group.

Note: Fast-leave processing is supported only with MLD version 1 hosts.

Default	disabled
Format	`set mld fast-leave` *`vlan-id`*
Mode	Interface Config VLAN Mode

no set mld fast-leave

Use this command to disable MLD Snooping fast-leave admin mode on a selected interface.

Format	`no set mld fast-leave` *`vlan-id`*
Mode	Interface Config VLAN Mode

set mld groupmembership-interval

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	`set mld groupmembership-interval` *`vlan-id seconds`*
Mode	Interface Config Global Config VLAN Mode

no set groupmembership-interval

Use this command to set the MLDv2 group membership Interval time to the default value.

Format	`no set mld groupmembership-interval`
Mode	Interface Config Global Config VLAN Mode

set mld maxresponse

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	`set mld maxresponse` *`seconds`*
Mode	Global Config Interface Config 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 VLAN Mode

set mld mcrtexpiretime

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 mcrtexpiretime` *`vlan-id seconds`*
Mode	Global Config Interface Config

no set mld mcrtexpiretime

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 mcrtexpiretime` *`vlan-id`*
Mode	Global Config Interface Config

set mld mrouter

Use this command to configure the VLAN ID for the VLAN that has the multicast router attached mode enabled.

Format	`set mld mrouter` *`vlan-id`*
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	`no set mld mrouter` *`vlan-id`*
Mode	Interface Config

set mld mrouter interface

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	`set mld mrouter interface`
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	`no set mld mrouter interface`
Mode	Interface Config

show mldsnooping

Use this command to display MLD Snooping information. Configured information is displayed whether or not MLD Snooping is enabled.

Format	`show mldsnooping [unit/slot/port | vlan-id]`
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.

When you specify the *unit/slot/port* values, the following information displays.

Term	Definition
MLD Snooping Admin Mode	Indicates whether MLD Snooping is active on the interface.
Fast Leave Mode	Indicates whether MLD Snooping Fast Leave is active on the VLAN.
Group Membership Interval	Shows 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.
Max Response Time	Displays 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 Present Expiration Time	Displays 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.

When you specify a value for *vlan-id*, the following information displays.

Term	Definition
VLAN Admin Mode	Indicates whether MLD Snooping is active on the VLAN.

show mldsnooping mrouter interface

Use this command to display information about statically configured multicast router attached interfaces.

Format	`show mldsnooping mrouter interface` *`unit/slot/port`*
Mode	Privileged EXEC

Term	Definition
Interface	Shows the interface on which multicast router information is being 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

Use this command to display information about statically configured multicast router-attached interfaces.

Format	`show mldsnooping mrouter vlan` *`unit/slot/port`*
Mode	Privileged EXEC

Term	Definition
Interface	Shows the interface on which multicast router information is being displayed.
VLAN ID	Displays the list of VLANs of which the interface is a member.

show mldsnooping ssm entries

Use this command to display the source specific multicast forwarding database built by MLD snooping.

A given 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	`show mldsnooping ssm entries`
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.

Term	Definition
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 mldsnooping ssm stats

Use this command to display the statistics of MLD snooping’s SSMFDB. This command takes no options.

Format	`show mldsnooping ssm stats`
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 mldsnooping ssm groups

Use this command to display the MLD SSM group membership information.

Format	`show mldsnooping 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 mldsnooping

Use this command to display the MLD Snooping entries in the Multicast Forwarding Database (MFDB) table.

Format	`show mac-address-table mldsnooping`
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 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 mldsnooping

Use this command to delete all MLD snooping entries from the MFDB table.

Format	`clear mldsnooping`
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 system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

set mld querier

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	`set mld querier [`*`vlan-id`*`] [address `*`ipv6-address`*`]`
Mode	Global Config 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	`no set mld querier [`*`vlan-id`*`] [address]`
Mode	Global Config VLAN Mode

set mld querier query_interval

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	`set mld querier query_interval `*`seconds`*
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

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` *`seconds`*
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

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`
Mode	VLAN Config

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`
Mode	VLAN Config

show mldsnooping querier

Use this command to display MLD Snooping Querier information. Configured information is displayed whether or not MLD Snooping Querier is enabled.

Format	`show mldsnooping querier [detail | vlan` *`vlan-id`*`]`
Mode	Privileged EXEC

When 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.

When 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.
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 argument **detail** is used, the command shows the global information and the information for all Querier-enabled VLANs.

set mld proxy-querier

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, on a particular VLAN and all interfaces participating in the VLAN.

By default, the proxy-querier is enabled.

Default	enabled
Format	`set mld proxy-querier [vlan-id]`
Mode	Global Config Interface Config VLAN Config

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, on a particular VLAN and all interfaces participating in the VLAN.

This command is specific to MLD.

Format	`no set mld proxy-querier [vlan-id]`
Mode	Global Config Interface Config VLAN Config

show mldsnooping proxy-querier

This command shows the global admin mode of the MLD snooping proxy-querier and the interface on which it is enabled.

Format	`show mldsnooping proxy-querier`
Mode	Privileged EXEC

Command example:

```
(Netgear Switch) #show mldsnooping 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 given 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 136.

port-security

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 max-dynamic

This command sets the maximum number of dynamically locked MAC addresses allowed on a specific port. The valid range is 0–600.

Default	600
Format	`port-security max-dynamic` *`maxvalue`*
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

This command sets the maximum number of statically locked MAC addresses allowed on a port. The valid range is 0–20.

Default	1
Format	`port-security max-static` *`maxvalue`*
Mode	Interface Config

no port-security max-static

This command sets maximum number of statically locked MAC addresses to the default value.

Format	`no port-security max-static`
Mode	Interface Config

port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses for an interface or range of interfaces. The *`vid`* is the VLAN ID.

Format	`port-security mac-address` *`mac-address vid`*
Mode	Interface Config

no port-security mac-address

This command removes a MAC address from the list of statically locked MAC addresses.

Format	`no port-security mac-address` *`mac-address vid`*
Mode	Interface Config

port-security mac-address move

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

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 *vid* 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 vid`* entries. This distinguishes them from static entries.

Format	`port-security mac-address sticky [`*`mac-address vid`*`]`
Mode	Global Config 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 [`*`mac-address vid`*`]`
Mode	Global Config Interface Config

show port-security

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. 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 [`*`unit/slot/port`*` | 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 Routing) #show port-security 0/1

        Admin    Dynamic     Static     Violation  Sticky
Intf    Mode      Limit      Limit      Trap Mode  Mode
------  -------  ----------  ---------  ---------  --------
0/1     Disabled    1          1        Disabled   Enabled
```

show port-security dynamic

This command displays the dynamically locked MAC addresses for the port. 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`*
Mode	Privileged EXEC

Term	Definition
MAC Address	MAC Address of dynamically locked MAC.

show port-security static

This command displays the statically locked MAC addresses for a port. 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

This command displays the source MAC address of the last packet discarded on a locked port. 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 violation {*unit/slot/port* | lag *lag-intf-num*}
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

Use this command to enable the LLDP advertise capability on an interface or a range of interfaces.

Default	disabled
Format	`lldp transmit`
Mode	Interface Config

no lldp transmit

Use this command to return the local data transmission capability to the default.

Format	`no lldp transmit`
Mode	Interface Config

lldp receive

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

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 1–32768 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` *`interval-seconds`*`] [hold` *`hold-value`*`] [reinit` *`reinit-seconds`*`]`
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

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 134. 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 358

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-mgmt

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

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

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` *`interval`*
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

clear lldp statistics

Use this command to reset all LLDP statistics, including MED-related information.

Format	`clear lldp statistics`
Mode	Privileged Exec

clear lldp remote-data

Use this command to delete all information from the LLDP remote data table, including MED-related information.

Format	`clear lldp remote-data`
Mode	Global Config

show lldp

Use this command to display a summary of the current LLDP configuration.

Format	`show lldp`
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

Use this command to display a summary of the current LLDP configuration for a specific interface or for all interfaces.

Format	`show lldp interface {`*`unit/slot/port`* `| all}`
Mode	Privileged Exec

Term	Definition
Interface	The interface in a *`unit/slot/port`* 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

Use this command to display the current LLDP traffic and remote table statistics for a specific interface or for all interfaces.

Format	`show lldp statistics {`*`unit/slot/port`* `| all}`
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 in *`unit/slot/port`* format.
TX Total	Total number of LLDP packets transmitted on the port.

Term	Definition
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

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.

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

Use this command to display detailed information about remote devices that transmit current LLDP data to an interface on the system.

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.

Term	Definition
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

Use this command to display summary information about the advertised LLDP local data. This command can display summary information or detail for each interface.

Format	`show lldp local-device {`*`unit/slot/port`*` | all}`
Mode	Privileged EXEC

Term	Definition
Interface	The interface in a *`unit/slot/port`* format.
Port ID	The port ID associated with this interface.
Port Description	The port description associated with the interface.

show lldp local-device detail

Use this command to display detailed information about the LLDP data a specific interface transmits.

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

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

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 ldp med confignotification

Use this command to disable notifications.

Format	`no lldp med confignotification`
Mode	Interface Config

lldp med transmit-tlv

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs) from this interface or a range of interfaces.

Default	By default, the capabilities and network policy TLVs are included.
Format	`lldp med transmit-tlv [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]`
Mode	Interface Config

Parameter	Definition
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

no lldp med transmit-tlv

Use this command to remove a TLV.

Format	`no lldp med transmit-tlv [capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]`
Mode	Interface Config

lldp med all

Use this command to configure LLDP-MED on all the ports.

Format	`lldp med all`
Mode	Global Config

lldp med confignotification all

Use this command to configure all the ports to send the topology change notification.

Format	`lldp med confignotification all`
Mode	Global Config

lldp med faststartrepeatcount

Use this command to set the value of the fast start repeat count. *count* is the number of LLDP PDUs that are transmitted when the product is enabled. The range is 1 to 10.

Default	3
Format	`lldp med faststartrepeatcount [`*count*`]`
Mode	Global Config

no lldp med faststartrepeatcount

Use this command to return to the factory default value.

Format	`no lldp med faststartrepeatcount`
Mode	Global Config

lldp med transmit-tlv all

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be 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] [ex-pd] [ex-pse] [inventory] [location] [network-policy]`
Mode	Global Config

Term	Definition
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

no lldp med transmit-tlv

Use this command to remove a TLV.

Format	`no lldp med transmit-tlv [capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]`
Mode	Global Config

show lldp med

Use this command to display a summary of the current LLDP MED configuration.

Format	`show lldp med`
Mode	Privileged Exec

Command example:

```
(NETGEAR Routing) #show lldp med
LLDP MED Global Configuration

Fast Start Repeat Count: 3
Device Class: Network Connectivity

(NETGEAR Routing) #
```

show lldp med interface

Use this command to display a summary of the current LLDP MED configuration for a specific interface. *unit/slot/port* indicates a specific physical interface; **all** indicates all valid LLDP interfaces.

Format	show lldp med interface {*unit/slot/port* | all}
Mode	Privileged Exec

Command example:

```
(NETGEAR Routing) #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
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
(NETGEAR Routing) #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

Use this command to display detailed information about the LLDP MED data that a specific interface transmits. *unit/slot/port* indicates a specific physical interface.

Format	show lldp med local-device detail *unit/slot/port*
Mode	Privileged EXEC

Command example:

```
(NETGEAR Routing) #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

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 valid LLDP interfaces or on a specific physical interface.

Format	`show lldp med remote-device {`*`unit/slot/port`* `| 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 Routing) #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

Use this command to display detailed information about remote devices that transmit current LLDP MED data to an interface on the system.

Format	`show lldp med remote-device detail` *unit/slot/port*
Mode	Privileged EXEC

Command example:

```
(NETGEAR Routing) #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. NETGEAR Managed Switch software 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 then 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

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

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 will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control sipdip`
Mode	Global Config

no dos-control sipdip

This command disables Source IP address = Destination IP address (SIP = DIP) Denial of Service prevention.

Format	`no dos-control sipdip`
Mode	Global Config

dos-control firstfrag

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 having a TCP Header Size smaller then the configured value, the packets will be dropped if the mode is enabled. The default is disabled. The range is 0–255. If you enable dos-control firstfrag, but do not provide a Minimum TCP Header Size, the system sets that value to 20.

Default	disabled (20)
Format	`dos-control firstfrag [`*`size`*`]`
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	`no dos-control firstfrag`
Mode	Global Config

dos-control tcpfrag

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 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 are dropped.

Default	disabled
Format	`dos-control tcpfrag`
Mode	Global Config

no dos-control tcpfrag

This command disables TCP Fragment Denial of Service protection.

Format	`no dos-control tcpfrag`
Mode	Global Config

dos-control tcpflag

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 packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpflag`
Mode	Global Config

no dos-control tcpflag

This command sets disables TCP Flag Denial of Service protections.

Format	`no dos-control tcpflag`
Mode	Global Config

dos-control l4port

This command enables L4 Port Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having Source TCP/UDP Port Number equal to Destination TCP/UDP Port Number, the packets will be dropped if the mode is enabled.

Note: Some applications mirror source and destination L4 ports - RIP for example uses 520 for both. If you enable dos-control l4port, applications such as RIP may experience packet loss which would render the application inoperable.

Default	disabled
Format	`dos-control l4port`
Mode	Global Config

no dos-control l4port

This command disables L4 Port Denial of Service protections.

Format	`no dos-control l4port`
Mode	Global Config

dos-control smacdmac

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 will be 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

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 will be 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

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 will be 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

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 packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpflagseq`
Mode	Global Config

no dos-control tcpflagseq

This command sets disables TCP Flag and Sequence Denial of Service protection.

Format	`no dos-control tcpflagseq`
Mode	Global Config

dos-control tcpoffset

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 having TCP Header Offset equal to one (1), the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpoffset`
Mode	Global Config

no dos-control tcpoffset

This command disabled TCP Offset Denial of Service protection.

Format	`no dos-control tcpoffset`
Mode	Global Config

dos-control tcpsyn

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 having TCP flag SYN set and an L4 source port from 0 to 1023, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpsyn`
Mode	Global Config

no dos-control tcpsyn

This command sets disables TCP SYN and L4 source = 0-1023 Denial of Service protection.

Format	`no dos-control tcpsyn`
Mode	Global Config

dos-control tcpsynfin

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 having TCP flags SYN and FIN set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpsynfin`
Mode	Global Config

no dos-control tcpsynfin

This command sets disables TCP SYN & FIN Denial of Service protection.

Format	`no dos-control tcpsynfin`
Mode	Global Config

dos-control tcpfinurgpsh

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 having TCP FIN, URG, and PSH all set and TCP Sequence Number set to 0, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpfinurgpsh`
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	`no dos-control tcpfinurgpsh`
Mode	Global Config

dos-control icmpv4

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	`dos-control icmpv4 [`*`size`*`]`
Mode	Global Config

no dos-control icmpv4

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	`no dos-control icmpv4`
Mode	Global Config

dos-control icmpv6

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 having a size greater than the configured value, the packets will be dropped if the mode is enabled. The value for the size is from 0–16376.

Default	disabled (512)
Format	`dos-control icmpv6 [size]`
Mode	Global Config

no dos-control icmpv6

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	`no dos-control icmpv6`
Mode	Global Config

dos-control icmpfrag

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 packets ingress having fragmented ICMP packets, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control icmpfrag`
Mode	Global Config

no dos-control icmpfrag

This command disabled ICMP Fragment Denial of Service protection.

Format	`no dos-control icmpfrag`
Mode	Global Config

show dos-control

This command displays Denial of Service configuration information.

Format	`show dos-control`
Mode	Privileged EXEC

Term	Definition
First Fragment Mode	The administrative mode of First Fragment DoS prevention. When enabled, this causes the switch to drop packets that have a TCP header smaller then the configured Min TCP Hdr Size.
Min TCP Hdr Size	The minimum TCP header size the switch will accept if First Fragment DoS prevention is enabled.
ICMPv4 Mode	The administrative mode of ICMPv4 DoS prevention. When enabled, this causes the switch to drop 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 to accept when ICMPv4 DoS protection is enabled.
ICMPv6 Mode	The administrative mode of ICMPv6 DoS prevention. When enabled, this causes the switch to drop 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 to accept when ICMPv6 DoS protection is enabled.
ICMPv4 Fragment Mode	The administrative mode of ICMPv4 Fragment DoS prevention. When enabled, this causes the switch to drop fragmented ICMPv4 packets.
TCP Port Mode	The administrative mode of TCP Port DoS prevention. When enabled, this causes the switch to drop packets that have the TCP source port equal to the TCP destination port.
UDP Port Mode	The administrative mode of UDP Port DoS prevention. When enabled, this causes the switch to drop packets that have the UDP source port equal to the UDP destination port.
SIPDIP Mode	The administrative mode of SIP=DIP DoS prevention. Enabling this causes the switch to drop packets that have a source IP address equal to the destination IP address. The factory default is disabled.
SMACDMAC Mode	The administrative mode of SMAC=DMAC DoS prevention. Enabling this causes the switch to drop 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. Enabling this causes the switch to drop packets that have TCP flags FIN, URG, and PSH set and TCP Sequence Number = 0.
TCP Flag & Sequence Mode	The administrative mode of TCP Flag DoS prevention. Enabling this causes the switch to drop packets that have TCP control flags set to 0 and TCP sequence number set to 0.
TCP SYN Mode	The administrative mode of TCP SYN DoS prevention. Enabling this causes the switch to drop packets that have TCP Flags SYN set.
TCP SYN & FIN Mode	The administrative mode of TCP SYN & FIN DoS prevention. Enabling this causes the switch to drop packets that have TCP Flags SYN and FIN set.

Term	Definition
TCP Fragment Mode	The administrative mode of TCP Fragment DoS prevention. Enabling this causes the switch to drop 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. Enabling this causes the switch to drop packets that have a TCP header Offset equal to 1.

MAC Database Commands

This section describes the commands you use to configure and view information about the MAC databases.

bridge aging-time

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. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered.

Default	300
Format	`bridge aging-time` *seconds*
Mode	Global Config

no bridge aging-time

This command sets the forwarding database address aging timeout to the default value. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered.

Format	`no bridge aging-time`
Mode	Global Config

show forwardingdb agetime

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

This command displays the Multicast Forwarding Database (MFDB) information. If you enter the command with no parameter, 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` *macaddr*
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

                                                                  Fwd
VLAN ID MAC Address       Source  Type    Description     Interface 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

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

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

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` *`seconds`*
Mode	Global Config

isdp timer

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	`isdp timer` *`seconds`*
Mode	Global Config

isdp advertise-v2

This command enables the sending of ISDP version 2 packets from the device.

Default	Enabled
Format	`isdp advertise-v2`
Mode	Global Config

no isdp advertise-v2

This command disables the sending of ISDP version 2 packets from the device.

Format	`no isdp advertise-v2`
Mode	Global Config

isdp enable

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 609.

Default	Enabled
Format	`isdp enable`
Mode	Interface Config

no isdp enable

This command disables ISDP on the interface.

Format	`no isdp enable`
Mode	Interface Config

clear isdp counters

This command clears ISDP counters.

Format	`clear isdp counters`
Mode	Privileged EXEC

clear isdp table

This command clears entries in the ISDP table.

Format	`clear isdp table`
Mode	Privileged EXEC

show isdp

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 given in seconds.
Hold Time	The length of time the receiving device should save information sent by this device. This value is given 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 Routing) #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

This command displays ISDP settings for the specified interface.

Format	`show isdp interface {all | `*`unit/slot/port`*`}`
Mode	Privileged EXEC

Term	Definition
Interface	The *unit/slot/port* 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

This command displays ISDP entries. If the *device-id* is specified, then only entries for that device are shown.

Format	`show isdp entry {all | device-id}`
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.

Term	Definition
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 XCM8900
Interface                  0/1
Port ID                    GigabitEthernet1/1
Holdtime                   64
Advertisement              Version 2
Entry last changed time    0 days 00:13:50
```

show isdp neighbors

This command displays the list of neighboring devices.

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 (*`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.

Term	Definition
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

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

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

Term	Definition
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 Routing) #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

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

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)

This command enables UDLD globally on the switch.

Default	disable
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

This command configures the interval between UDLD probe messages on ports that are in the advertisement phase. The range is from 7 to 90 seconds.

Default	15 seconds
Format	`udld message time` *`seconds`*
Mode	Global Config

udld timeout interval

This command configures the time interval after which UDLD link is considered to be unidirectional. The range is from 5 to 60 seconds.

Default	5 seconds
Format	`udld timeout interval` *seconds*
Mode	Global Config

udld reset

This command resets all interfaces that have been shutdown by UDLD.

Default	None
Format	`udld reset`
Mode	Privileged EXEC

udld enable (Interface Config)

This command enables UDLD on the specified interface.

Default	disable
Format	`udld enable`
Mode	Interface Config

no udld enable (Interface Config)

This command disables UDLD on the specified interface.

Format	`no udld enable`
Mode	Interface Config

udld port

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

This command displays either the global settings of UDLD or the UDLD settings for the specified unit/slot/port. If the **all** keyword is entered, the command displays information for all ports.

Format	`show udld [unit/slot/port | all]`
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 Routing) #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 udld 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
```

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.

Note: These commands are supported on M6100 series switches only.

debounce-time

This command configures the debounce time. The possible values for the *milliseconds* parameter are in the 100–5000 range.

Format	`debounce-time` *`milliseconds`*
Mode	Interface Config

No debounce-time

This command disables the debounce time.

Format	`no debounce-time`
Mode	Interface Config

show interface debounce

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
```

Data Center Commands

9

The data center commands allow network operators to deploy lossless Ethernet capabilities in support of a converged network with Fiber Channel and Ethernet data, as specified by the FC-BB-5 working group of ANSI T11. This capability allows operators to deploy networks at a lower cost while still maintaining the same network management operations that exist today.

Note: Data center commands are supported on M6100 series switches only.

The chapter includes the following sections:

- *Data Center Bridging Exchange Protocol Commands*
- *Enhanced Transmission Selection and Traffic Class Group*
- *FIP Snooping Commands*
- *Priority-Based Flow Control Commands*

Data Center Bridging Exchange Protocol Commands

The Data Center Bridging Exchange Protocol (DCBX) is used by DCB devices to exchange configuration information with directly-connected peers. The protocol is also used to detect misconfiguration of the peer DCB devices and, optionally, for configuration of peer DCB devices.

lldp dcbx version

Use the **lldp dcbx version** command in Global Configuration mode to configure the administrative version for the Data Center Bridging Capability Exchange (DCBX) protocol. This command enables the switch to support a specific version of the DCBX protocol or to detect the peer version and match it. DCBX can be configured to operate in IEEE mode or CEE mode or CIN. In **auto** mode, version detection is based on the peer device DCBX version. The switch operates in either IEEE or one of the legacy modes on each interface.

In **auto** mode, the switch will attempt to jump start the exchange by sending an IEEE frame, followed by a CEE frame followed by a CIN frame. The switch will parse the received response and immediately switch to the peer version.

Note: CIN is Cisco® Intel® Nuova DCBX (version 1.0). CEE is converged enhanced Ethernet DCBX (version 1.06).

Default	auto
Format	`lldp dcbx version {auto | cin | cee | ieee}`
Mode	Global Config

Parameter	Description
auto	Automatically select the version based on the peer response.
cin	Force the mode to Cisco-Intel-Nuova. (DCBX 1.0)
cee	Force the mode to CEE (DCBX 1.06)
ieee	Force the mode to IEEE 802.1Qaz

Command example:

The following example configures the switch to use CEE DCBX:

```
s1(config)#lldp dcbx version cee
```

no lldp dcbx version

Use the no form of the command to reset the DCBX version to the default value of auto.

Format	`no lldp dcbx version`
Mode	Global Config

lldp tlv-select dcbxp

Use the **`lldp tlv-select dcbxp`** command in Interface Configuration or Global Configuration mode to send specific DCBX TLVs if LLDP is enabled to transmit on the given interface. If no parameter is given, all DCBX TLVs are enabled for transmission. The default is all DCBX TLVs are enabled for transmission. If executed in Interface mode, the interface configuration overrides the global configuration on the designated interface. Entering the command with no parameters enables transmission of all TLVs.

Default	Transmission of all TLVs is enabled by default.
Format	`lldp tlv-select dcbxp [ets-config | ets-recommend | pfc | application-priority]`
Mode	• Interface Config • Global Config

Parameter	Description
ets-config	Transmit the ETS configuration TLV.
ets-recommend	Transmit the ETS recommendation TLV.
pfc	Transmit the PFC configuration TLV.
application-priority	Transmit the application priority TLV.

no lldp tlv-select dcbxp

Use the **`no lldp tlv-select dcbxp`** command to disable LLDP from sending all or individual DCBX TLVs, even if LLDP is enabled for transmission on the given interface.

Format	`no lldp tlv-select dcbxp [ets-config | ets-recommend | pfc | application-priority]`
Mode	• Interface Config • Global Config

Command example:

The following example configures the port to transmit all TLVs:

```
console(interface-config)#no lldp tlv-select dcbxp
```

lldp dcbx port-role

Use the **lldp dcbx port-role** command in Interface Configuration mode to configure the port role to manual, auto-upstream, auto-downstream and configuration source. In order to reduce configuration flapping, ports that obtain configuration information from a configuration source port will maintain that configuration for 2x the LLDP timeout, even if the configuration source port becomes operationally disabled.

Default	The default port role is manual.
Format	`lldp dcbx port-role {auto-up |auto-down | manual | configuration-source}`
Mode	Interface Config

Parameter	Description
Manual	Ports operating in the manual role do not have their configuration affected by peer devices or by internal propagation of configuration. These ports will advertise their configuration to their peer if DCBX is enabled on that port. The willing bit is set to disabled on manual role ports.
Auto-up	Advertises a configuration, but is also willing to accept a configuration from the link-partner and propagate it internally to the auto-downstream ports as well as receive configuration propagated internally by other auto-upstream ports. These ports have the willing bit enabled. These ports should be connected to FCFs.
Auto-down	Advertises a configuration but is not willing to accept one from the link partner. However, the port will accept a configuration propagated internally by the configuration source. These ports have the willing bit set to disabled. Selection of a port based upon compatibility of the received configuration is suppressed. These ports should be connected to a trusted FCF.
Configuration Source	In this role, the port has been manually selected to be the configuration source. Configuration received over this port is propagated to the other auto-configuration ports. Selection of a port based upon compatibility of the received configuration is suppressed. These ports should be connected to a trusted FCF. These ports have the willing bit enabled.

Command example:

The following example configures an FCF facing port:

```
console(config-if-Te1/1/1)#lldp dcbx port-role auto-up
```

Command example:

The following example configures an FCoE host facing port:

```
console(config-if-Te1/1/1)#lldp dcbx port-role auto-down
```

no lldp dcbx port-role

Use the **no lldp dcbx port-role** command in Interface Configuration mode to configure the port role to manual.

Format	no lldp dcbx port-role
Mode	Interface Config

show lldp tlv-select

Use the **show lldp tlv-select** command in Privileged EXEC mode to display the per interface TLV configuration.

Format	show lldp tlv-select {interface all | *unit/slot/port*}
Mode	Privileged EXEC

Parameter	Description
all	All interfaces.
unit/slot/port	A valid physical interface specifier.

Command example:

The following command shows the TLVs selected for transmission on multiple interfaces:

```
switch(config)# show lldp tlv-select interface all

Interface      ETS Config  ETS Recommend  PFC  App Priority QCN
-------------- ----------  -------------  ---  ------------ ---
te1/0/1            Yes           No       Yes  No           Yes
te1/0/2            No            No       Yes  No           Yes
```

show lldp dcbx interface

Use the **show lldp dcbx interface** command in Privileged EXEC mode to display the local DCBX control status of an interface.

Format	show lldp dcbx {interface all | *unit/slot/port*} [detail]
Mode	Privileged EXEC

Parameter	Description
unit/slot/port	A valid physical interface specifier.
all	All interfaces.
Detail	Display detailed DCBX information.

Command example:

The following output shows DCBX status:

```
(NETGEAR Routing) #show lldp dcbx interface all

Is configuration source selected.............. False

                                                DCBX   DCBX  DCBX    unknown
Interface  Status     Role          Version    Tx     Rx    Errors  TLV
---------- ---------- ------------- --------- ------- ----- ------- -------
0/1        Disabled   Manual        Auto       0       0     0       0
0/2        Disabled   Manual        Auto       0       0     0       0
0/3        Disabled   Manual        Auto       0       0     0       0
0/4        Disabled   Manual        Auto       0       0     0       0
0/5        Disabled   Manual        Auto       0       0     0       0
0/6        Disabled   Manual        Auto       0       0     0       0
0/7        Disabled   Manual        Auto       0       0     0       0
0/8        Disabled   Manual        Auto       0       0     0       0
0/9        Disabled   Manual        Auto       0       0     0       0
0/10       Disabled   Manual        Auto       0       0     0       0
0/11       Disabled   Manual        Auto       0       0     0       0
0/12       Disabled   Manual        Auto       0       0     0       0
0/13       Disabled   Manual        Auto       0       0     0       0
0/14       Disabled   Manual        Auto       0       0     0       0
0/15       Disabled   Manual        Auto       0       0     0       0
0/16       Disabled   Manual        Auto       0       0     0       0
0/17       Disabled   Manual        Auto       0       0     0       0
```

Command example:

The following output shows that DCBX is not enabled:

```
switch(config)# show lldp dcbx interface te1/0/1
Interface te1/0/1
 DCBX Admin Status:                  Disabled
 Configured DCBX Version:            Auto
 Peer DCBX Version:
 Peer MAC:
 Peer Description:
 Auto-configuration Port Role:       Manual
 Peer Is Configuration Source:       False

Error Counters:
 ETS Incompatible Configuration: 0
 PFC Incompatible Configuration: 0
 Disappearing Neighbor:          0
 Multiple Neighbors Detected:    0
```

Command example:

The following output shows that DCBX is enabled with a legacy device (CIN/CEE):

```
switch(config)# show lldp dcbx interface te1/0/1
Interface te1/0/1
 DCBX Admin Status:                  Enabled
 Configured Version:                 Auto
 Peer DCBX Version:                  CIN Version 1.0
 Peer MAC:                           00:23:24:A4:21:03
 Peer Description:                   Cisco Nexus 5020 IOS Version 5.00
 Auto-configuration Port Role:       Auto-down
 Peer Is Configuration Source:       False

Local Configuration:

               Max/Oper
Type  Subtype  Version   En/Will/Adv
PFC(3) 000     000       Y/Y/Y
PG(2)  000     000       Y/Y/Y
APP(4) 000     000       Y/Y/Y

Number of TCs Supported: 3
Priority Group Id:    0:00 1:01 2:02  3:03  4:04  5:05  6:06  7:07
PG Percentage (%):    0:12 1:10 2:12  3:00  4:00  5:66  6:00  7:00
Strict Priority:      0:0  1:2  2:0   3:0   4:0   5:0   6:0   7:0
PFC Enable Vector:    0:0  1:1  2:0   3:0   4:0   5:0   6:0   7:0

Peer Configuration:

Operation version: 00  Max version: 00  Seq no: 23  Ack no: 22

               Max/Oper
Type   Subtype Version   En/Will/Err
PFC(3) 000     000/000   Y/N/N
PG(2)  000     000/000   Y/N/N
APP(4) 000     000/000   Y/N/N

Number of TCs Supported: 3
Priority Group Id:    0:00 1:01 2:02  3:03  4:04  5:05  6:06  7:07
PG Percentage (%):    0:0  1:10 2:12  3:00  4:00  5:78  6:00  7:00
PFC Enable Vector:    0:0  1:1  2:0   3:0   4:0   5:1   6:0   7:0

Application Priority (TX Enabled)
 Type         Application    Priority    Status
 -------------------------------------------------
 Ethernet     FC0E            3          Enabled
 TCP/SCTP     860             4          Disabled
```

```
 TCP/SCTP     3260            4          Disabled

Error Counters:
 ETS Incompatible Configuration: 0
 PFC Incompatible Configuration: 0
 Disappearing Neighbor:          0
 Multiple Neighbors Detected:    0
```

Command example:

The following output shows that DCBX is enabled with an IEEE device (DCBX Version Forced):

```
switch(config)# show lldp dcbx interface te1/0/1
Interface te1/0/1
 DCBX Admin Status:                  Enabled
 Configured DCBX Version:            CIN 1.0
 Peer DCBX Version:                  CEE 1.6
 Peer MAC:                           00:23:24:A4:21:03
 Peer Description:                   Cisco Nexus 5020 IOS Version 5.00
 Auto-configuration Port Role:       Auto-upstream
 Peer Is Configuration Source:       True

Error Counters:
 ETS Incompatible Configuration: 7
 PFC Incompatible Configuration: 0
 Disappearing Neighbor:          0
 Multiple Neighbors Detected:    0
```

Command example:

The following output shows that DCBX is enabled and provides a detailed view with the transmitted and received TLV information. The ETS information is documented in IEEE 802.1az D2.4, tables D-2, D-3, and D-4. The PFC Enable Vector information is documented in IEEE 802.1az D2.4, table D-5. The transmitted recommendation TLV is never displayed because it is always the same as the configured TLV. The peer description is obtained from the LLDP System Name.

```
switch(config)# show lldp dcbx interface te1/0/1 detail
Interface te1/0/1
 DCBX Admin Status:                  Enabled
 Configured Version:                 Auto
 Auto-configuration Port Role:       Configuration Source
 Peer Is Configuration Source:       True

PFC Capability (TX Enabled)
 Willing: True     MBC: False  Max PFC classes supported: 3
 PFC Enable Vector:       0:0 1:1 2:0 3:0 4:0 5:1 6:0 7:0
```

```
ETS Configuration (TX Enabled)
 Willing: True    Credit Shaper: False  Traffic Classes Supported: 3
 Priority Assignment:          0:0  1:1  2:2  3:3  4:4  5:5  6:6  7:7
 Traffic Class Bandwidth (%):  0:00 1:10 2:12 3:00 4:00 5:78 6:00 7:00
 Traffic Selection Algorithm:  0:0  1:1  2:3  3:0  4:0  5:3  6:0  7:0
ETS Recommendation (TX Enabled)

Peer DCBX Version:             CEE 1.6
Peer Description:              Cisco Nexus 5020 IOS Version 5.00
Peer MAC:                      00:23:24:A4:21:03
Peer PFC Capability:
 Willing: False   MBC: False   Max PFC classes supported: 3
 PFC Enable Vector       0:0 1:1 2:0 3:0 4:0 5:1 6:0 7:0
Peer ETS Configuration:
 Willing: False  Peer ETS Detected: True  Credit Shaper: False
 Traffic Classes Supported:    8
 Priority Assignment:          0:0  1:1  2:1  3:0  4:0  5:1  6:0  7:0
 Traffic Class Bandwidth:      0:00 1:10 2:12 3:00 4:00 5:78 6:00 7:00
 Traffic Selection Algorithm:  0:0  1:1  2:3  3:0  4:0  5:3  6:0  7:0
Peer ETS Recommendation:
 Traffic Class Bandwidth:      0:0  1:1  2:12 3:0  4:0  5:3  6:0  7:0
 Traffic Selection Algorithm:  0:0  1:1  2:3  3:0  4:0  5:3  6:0  7:0

Peer Application Priority
 Type         Application     Priority
 -------------------------------------
 Ethernet     0x8906           3
 TCP/SCTP     3260             4
```

Enhanced Transmission Selection and Traffic Class Group

classofservice traffic-class-group

Use the **classofservice traffic-class-group** command in Global Config or Interface Config mode to map the internal Traffic Class Group (TCG).

Default	All traffic classes are mapped to TCG 0.
Format	`classofservice traffic-class-group` *`trafficclass traffic-class-group`*
Mode	Global Config Interface Config

Parameter	Description
trafficclass	The Traffic Class can range from 0–6, although the actual number of available traffic classes depends on the platform.
traffic-class-group	The Traffic Class Group can range from 0–6, although the actual number of available traffic classes depends on the platform.

no classofservice traffic-class-group

Use the **no classofservice traffic-class-group** command in Global Config or Interface Config mode to restore the default mapping for each of the traffic classes.

Format	no classofservice traffic-class-group
Mode	Global Config Interface Config

traffic-class-group max-bandwidth

Use the **traffic-class-group max-bandwidth** command in Global Config or Interface Config mode to specify the maximum transmission bandwidth (bw) limit for each Traffic Class Group (TCG). Also known as rate shaping, this has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded. The total number of TCG supported per interface is platform specific.

Default	Max-bandwidth is zero for all TCG.
Format	traffic-class-group max-bandwidth *bw-0 bw-1 … bw-n*
Mode	Global Config Interface Config

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

Each *bw-x* value is a percentage that ranges from 0 to 100 in increments of 1. All n bandwidth values must be specified with this command, and each is independent of the others. The number n is platform-dependent and corresponds to the number of supported traffic classes groups. The default maximum bandwidth value for each TCG is 0, meaning no upper limit is enforced, which allows the TCG queue to consume any available nonguaranteed bandwidth of the interface.

If a nonzero value is specified for any bw-x maximum bandwidth parameter, it must not be less than the current minimum bandwidth value for the corresponding queue. A *bw-x* maximum bandwidth parameter value of 0 may be specified at any time without restriction.

The maximum bandwidth limits may be used with either a weighted or strict priority scheduling scheme.

Note: A value of 0 (the default) implies an unrestricted upper transmission limit, which is similar to 100%, although there may be subtle operational differences depending on how the device handles a *no limit* case versus *limit to 100%*.

no traffic-class-group max-bandwidth

Use the **`no traffic-class-group max-bandwidth`** command in Global Config or Interface Config mode to restore the default for each queue's maximum bandwidth value.

Format	`no traffic-class-group max-bandwidth`
Mode	Global Config Interface Config

traffic-class-group min-bandwidth

Use the **`traffic-class-group min-bandwidth`** command in Global Config or Interface Config mode to specify the minimum transmission bandwidth (bw) guarantee for each interface TCG. The total number of TCG supported per interface is platform specific.

Default	Min-bandwidth is zero for all TCG.
Format	`traffic-class-group min-bandwidth` *`bw-0 bw-1 … bw-n`*
Mode	Global Config Interface Config

The command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The Interface Config mode command is only available on platforms that support independent per-port class-of-service queue configuration.

Each bw-x value is a percentage that ranges from 0 to 100 in increments of 1. All n bandwidth values must be specified with this command, and their combined sum must not exceed 100%. The number n is platform dependent and corresponds to the number of supported Traffic Class Groups. The default minimum bandwidth value for each TCG is 0, meaning no bandwidth is guaranteed (best effort).

If the value of any bw-x minimum bandwidth parameter is specified as greater than the current maximum bandwidth value for the corresponding TCG, then its corresponding maximum bandwidth automatically increases the maximum to the same value.

no traffic-class-group min-bandwidth

Use the **no traffic-class-group min-bandwidth** command in Global Config or Interface Config mode to restore the default for each queue's minimum bandwidth value.

Format	`no traffic-class-group min-bandwidth`
Mode	Global Config Interface Config

traffic-class-group strict

Use the **traffic-class-group strict** command in Global Config or Interface Config mode to activate the strict priority scheduler mode for each specified TCG.

Default	Weighted scheduler mode is used for all TCG
Format	`traffic-class-group strict` *tcg-id-0* [*tcg-id-1* … *tcg-id-n*]
Mode	Global Config Interface Config

The command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The Interface Config mode command is only available on platforms that support independent per-port class-of-service queue configuration.

At least one, but no more than *n*, tcg-id values are specified with this command. Duplicate tcg-id values are ignored. Each tcg-id value ranges from 0 to (n-1), where n is the total number of TCG supported per interface. The number n is platform dependent and corresponds to the number of supported Traffic Class Groups.

When strict priority scheduling is used for a TCG, the minimum bandwidth setting for the TCG is ignored and packets are scheduled for transmission as soon as they arrive. A maximum bandwidth setting for the queue, if configured, serves to limit the outbound transmission rate of a strict priority TCG queue so that it does not consume the entire capacity of the interface. If multiple TCG on the same interface are configured for strict priority mode, the method of handling their packet transmission is platform specific. One typical scheme is to schedule all strict priority TCG ahead of the weighted queues, giving preference among the strict priority TCG to the one with the highest tcg-id.

no traffic-class-group strict

Use the **no traffic-class-group strict** command in Global Config or Interface Config mode to restore the default weighted scheduler mode for each specified TCG.

Format	`no traffic-class-group strict` *tcg-id-0* [*tcg-id-1* … *tcg-id-n*]
Mode	Global Config Interface Config

traffic-class-group weight

Use the **traffic-class-group weight** command in Global Config or Interface Config mode to specify the weight for each interface TCG. The total number of TCGs supported per interface is platform specific.

Default	For TCG0:TCG1:TCG2, weights are in the ratio 100%:0%:0%
Format	`traffic-class-group weight` *`wp-0 wp-1 … wp-n`*
Mode	Global Config Interface Config

The command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The Interface Config mode command is only available on platforms that support independent per-port class-of-service queue configuration.

Each wp-x (weight percentage) value is a percentage that ranges from 0 to 100 in increments of 1. All *n* bandwidth values must be specified with this command, and their combined sum must not exceed 100%. The number *n* is platform dependent and corresponds to the number of supported Traffic Class Groups. The default weight percentage value is in the ratio of 1:2:3 for TCG0:TCG1:TCG2, which is calculated as 100%:0%:0%.

The weight percentage is not considered for TCG that are configured for strict scheduling.

no traffic-class-group weight

Use the **no traffic-class-group weight** command in Global Config or Interface Config mode to restore the default for each queue's weight percentage value.

Format	`no traffic-class-group weight` *`wp-0 wp-1 … wp-n`*
Mode	Global Config Interface Config

show classofservice traffic-class-group

Use the **show classofservice traffic-class-group** command in Privileged EXEC mode to display the Traffic Class to Traffic Class Group mapping.

Format	`show classofservice traffic-class-group [`*`unit/slot/port`*`]`
Mode	Privileged EXEC

Parameter	Description
unit/slot/port	Optional and is only valid on platforms that support independent per-port class of service mappings. • If *unit/slot/port* is specified, the TCG mapping table of the interface is displayed. • If *unit/slot/port* is omitted, the global configuration settings are displayed (these may have been subsequently overridden by per-port configuration).
Traffic Class	The traffic class queue identifier.
Traffic Class Group	The traffic class Group identifier.

Command example:

```
(NETGEAR Routing) #show classofservice traffic-class-group

 Traffic Class    Traffic Class Group
 -------------    --------------------
   0     0
   1     1
   2     1
   3     1
   4     2
   5     1
   6     1
   7     1
```

FIP Snooping Commands

The Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) is used to perform the functions of FC_BB_E device discovery, initialization and maintenance. FIP uses a separate EtherType from FCoE to enable the distinction of discovery, initialization, and maintenance traffic from other FCoE traffic. FIP frames (with one exception) are the standard Ethernet size (1518 Byte 802.1q frame) whereas FCoE frames are a maximum of 2240 bytes.

This document describes FIP snooping, which is a frame inspection method used by FIP Snooping Bridges to monitor FIP frames and apply policies based upon the L2 header information in those frames, following recommendations in Annex C of FC_BB_5 Rev 2.00. This allows for:

1. Auto-configuration of Ethernet ACLs based on information in the Ethernet headers of FIP frames.
2. Emulation of FC point-to-point links within the DCB Ethernet network.
3. Enhanced FCoE security/robustness by preventing FCoE MAC spoofing.

The FIP Snooping Bridge solution in NETGEAR Managed Switch supports configuration-only of perimeter port role and FCF-facing port roles and is only intended for use at the edge of the switched network.

The role of FIP Snooping-enabled ports on the switch falls under one of the following types:

1. Perimeter or Edge port (connected directly to ENode).
2. FCF facing port (that receives traffic from FCFs targeted to the ENodes).

The default port role in an FCoE enabled VLAN is as a perimeter port. FCF facing ports must be configured by the user.

feature fip-snooping

Use the **`feature fip-snooping`** command in Global Configuration mode to globally enable Fibre Channel over Ethernet Initialization Protocol (FIP) snooping on the switch. When FIP snooping is disabled, received FIP frames are forwarded or flooded using the normal multicast rules.

When FIP snooping is enabled, FC-BB-5 Annex D ACLs are installed on the switch and FIP frames are snooped. FIP snooping will not allow FIP or Fiber Channel over Ethernet (FCoE) frames to be forwarded over a port until the port is operationally enabled for PFC. VLAN tagging must be enabled on the interface in order to carry the dot1p values through the network.

Default	disabled
Format	`feature fip-snooping`
Mode	Global Config

Command example:

The following example enables the FIP snooping feature:

```
s1(config)#feature fip-snooping
```

no feature fip-snooping

Use this command to return the settings to the default values and globally disable FIP snooping. When FIP snooping is globally disabled, received FIP frames are forwarded or flooded using the normal multicast rules. In addition, other FIP snooping commands are not available until the FIP snooping feature is enabled.

Format	`no feature fip-snooping`
Mode	Global Config

Command example:

The following example disables the FIP snooping feature:

```
s1(config)#no feature fip-snooping
```

fip-snooping enable

Use the **fip-snooping enable** command in VLAN Configuration mode to enable snooping of FIP packets on the configured VLANs. FIP snooping is disabled on VLANs by default.

Priority Flow Control (PFC) must be operationally enabled before FIP snooping can operate on an interface. VLAN tagging must be enabled on the interface in order to carry the dot1p value through the network.

This command can only be entered after FIP snooping is enabled using the *priority-flow-control mode* command. Otherwise, it does not appear in the CLI syntax tree.

Default	disabled
Format	`feature fip-snooping`
Mode	VLAN Config

Command example:

The following example enables FIP snooping on VLANs 2 through 8:

```
s1(config)#vlan 2-8
s1(config-vlan)#fip-snooping enable
```

no fip-snooping enable

Use this command to return the mode to the default (off).

Format	`no feature fip-snooping`
Mode	VLAN Config

Command example:

The following example disables FIP snooping on VLANs 2 through 8.

```
s1(config)#vlan 2-8
s1(config)(vlan 2-8)#no fip-snooping enable
s1(config)(vlan 2-8)# exit
```

fip-snooping fc-map

Use the **fip-snooping fc-map** command in VLAN Configuration mode to configure the FP-MAP value on a VLAN. The FC map value is used to help in securing the switch against misconfiguration.

When configured using fabric-provided MAC addresses, FCoE devices transmit frames containing the FC map value in the upper 24 bits. Only frames that match the configured FC map value are passed across the VLAN. Frames with MAC addresses that do not match the FC map value are discarded.

This command can only be entered after FIP snooping is enabled using the *priority-flow-control mode* command. Otherwise, it does not appear in the CLI syntax tree.

Default	The default FC map value is 0x0efc00.
Format	`fip-snooping fc-map` *`mapvalue`*
Mode	VLAN Config

Parameter	Description
map value	Valid FC map values are in the range of 0x0 to 0xffffff.

Command example:

The following example configures an FC map value of 0x100 on VLAN 208:

```
(config)# vlan 208
(config-vlan)# fip-snooping enable
(config-vlan)# fip-snooping fc-map 0x100
```

Command example:

The following example configures an FC value of 0xFFCB for VLAN range 2 through 8:

```
(config)# vlan 2-8
(config)(vlan 2-8)# fip-snooping fc-map 0xecffcb
(config)(vlan 2-8)# exit
```

no fip-snooping fc-map

This command sets the FC-MAP value for the VLAN to the default value.

Format	`no fip-snooping fc-map`
Mode	VLAN Config

fip-snooping port-mode

To relay the FIP packets received from the hosts toward the Fibre Channel Fabric (FCF), the switch needs to know the interfaces to which the FCFs are connected. Use the **`fip-snooping port-mode`** command in Interface Configuration mode to configure the interface that is connected towards FCF. By default, an interface is configured to be a host-facing interface if it is not configured to be an FCF-facing interface.

It is recommended that FCF-facing ports be placed into auto-upstream mode in order to receive DCBX information and propagate it to the CNAs on the downstream (host-facing) ports.

Interfaces enabled for PFC should be configured in trunk or general mode and must be PFC-operationally enabled before FCoE traffic can pass over the port.

This command can only be entered after FIP snooping is enabled using the *priority-flow-control mode* command. Otherwise, it does not appear in the CLI syntax tree.

Default	Configuration as a host-facing interface.
Format	`fip-snooping port-mode fcf`
Mode	Interface Config

Parameter	Description
fcf	Fibre Channel Fabric

Command example:

The following example configures an interface to be connected to an FCF switch:

```
(Config)# interface 1/0/1
(Interface 1/0/1)# fip-snooping port-mode fcf
(Interface 1/0/1)# exit
```

no fip-snooping port-mode

Use this command to set the interface to be connected towards the host.

Format	`no fip-snooping port-mode`
Mode	Interface Config

Command example:

The following example sets the interface to be connected towards the host:

```
(Config)# interface 1/0/1
(Interface 1/0/1)# no fip-snooping port-mode fcf
(Interface 1/0/1)# exit
```

show fip-snooping

Use the **`show fip-snooping sessions`** command in User EXEC or Privileged EXEC mode to display information about the global FIP snooping configuration and status.

Format	`show fip-snooping`
Mode	User EXEC Privileged EXEC

The following information is displayed.

Parameter	Description
Global Mode	FIP snooping configuration status on the switch. It displays Enable when FIP snooping is enabled on the switch and Disable when FIP snooping is disabled on the switch.
FCoE VLAN List	List of VLAN IDs on which FIP snooping is enabled.
FCFs	Number of FCFs discovered on the switch.
ENodes	Number of Enodes discovered on the switch.
Sessions	Total virtual sessions on the switch.
Max VLANs	Maximum number of VLANs that can be enabled for FIP snooping on the switch.
Max FCFs in VLAN	Maximum number of FCFs supported in a VLAN.
Max ENodes	Maximum number of ENodes supported in the switch.
Max Sessions	Maximum number of Sessions supported in the switch.

Command example:

```
(NETGEAR Switch)# show fip-snooping

Global Mode:   Enable
FCoE VLAN List :   2,4,5-8
FCFs:                    2
ENodes:                  2
Sessions:               10
Max VLANs:               8
Max FCFs in VLAN:        4
Max ENodes:            312
Max Sessions:         1024
```

show fip-snooping enode

Use the **show fip-snooping enode** command in User EXEC or Privileged EXEC mode to display information about the interfaces connected to ENodes.

Note: This command can only be entered after FIP snooping is enabled using the **feature fip-snooping** command. Otherwise, it does not appear in the CLI syntax tree.

Format	show fip-snooping enode [enode-mac]
Mode	User EXEC Privileged EXEC

Parameter	Description
enode-mac	MAC address of the enode to display.

The command displays the following information.

Parameter	Description
Interface	Interface to which the ENode is connected.
VLAN	ID number of the VLAN to which the ENode belongs.
NameID	Name of the ENode.
FIP-MAC	MAC address of the ENode.
FCID	Fiber channel ID number of the virtual port that was created by FCF when the ENode logged into the network.
Sessions Established	Number of successful virtual connections established.

The command displays the following additional information when the optional argument is supplied.

Parameter	Description
Sessions Waiting	Number of virtual connections waiting for FCF acceptance.
Sessions Failed	Number of virtual sessions failed.
Max-FCoE-PDU	Maximum FCoE PDU size the ENode MAC intends to use for FCoE traffic. This is equivalent to the maximum Ethernet frame payload the ENode intends to send.
Time elapsed	Time elapsed since first successful login session snooped from the ENode.

Command example:

The following output displays when you specify no optional argument:

```
(NETGEAR Switch)# show fip-snooping enode
Interface  VLAN  Name-ID          ENode-MAC      FCFs   Sessions
-----------------------------------------------------------------
1/0/2      1     00000000     00:0c:29:65:82:bc   1     3
1/0/5      100   00000000     00:0d:31:23:53:11   2     5
```

Command example:

The following output displays when you specify the optional argument:

```
(NETGEAR Switch)# show fip-snooping enode 00:0c:29:65:82:bc

Interface            1/0/2
```

```
VLAN                  1
Name-ID               000000
ENode-MAC             00:0c:29:65:82:bc
FCFs Connected        1
Sessions Established  3
Sessions Waiting      1
Session Failed        0
Max-FCoE-PDU          2158
Time elapsed          0 days, 1 hours, 20 minutes
```

show fip-snooping fcf

Use the **show fip-snooping fcf** command in User EXEC or Privileged EXEC mode to display information about the interfaces connected to FCFs.

Note: This command can only be entered after FIP snooping is enabled using the **feature fip-snooping** command. Otherwise, it does not appear in the CLI syntax tree.

Format	show fip-snooping fcf [fcf-mac]
Mode	User EXEC Privileged EXEC

The following information is displayed when no FCF mac argument is supplied.

Parameter	Description
Interface	Interface to which the FCF is connected.
VLAN	ID number of the VLAN to which the FCF belongs.
No. of ENodes	Total number of ENodes that are connected to the FCF.
FPMA/SPMA	Type of the MAC address for ENode as negotiated by the FCF.
FCMAP	FCMAP value used by the FCF.
FCF-MAC	MAC address of the FCF.
Fabric Name	Name of the FCF.

Below is additional information regarding the FCF that is displayed when the optional FCF MAC address argument is provided.

Parameter	Description
Sessions	Total number of virtual sessions accepted by FCF in the associated VLAN.
D-bit	This reflects the value of the D-bit provided by the most recently received Discovery Advertisement from the FCF. When D-bit value is zero then FIP snooping bridge verifies the periodic VN_Port FIP Keep Alive frames associated with FCF and Discovery Advertisements sent by FCF. When D-bit is set to 1, switch discards snooped VN_Port FIP Keep Alive frames associated with FCF and does not timeout the FCoE sessions established with the FCF based on FKA_VN_PERIOD*5 interval.
Available for Login	This reflects the value of the A bit provided by the most recently received Discovery Advertisement from the FCF. This provides the information that the transmitting FCF is available for FIP FLOGI/FDISC from ENodes. This is informational and shall have no effect on existing logins.
Priority	The Priority returned from the FCF in the Solicited Discovery Advertisement. This indicates the Priority that has been manually assigned to the FCF.
FKA-ADV	FIP keepalive interval (FKA_ADV_PERIOD) in seconds configured on the FCF multiplied by five. For example, if the FKA_ADV period configured on the FCF is 80 seconds, the value of this field is 400.
FCF Expiry Time	This is timer value to monitor the status of the FCF. FCF entry and all its associated virtual sessions will be removed when the value reaches 0. This value is reset to Configured FKA-ADV every time a Discovery Advertisement is received from the FCF-MAC.
Time Elapsed	Time since FCF is Discovered.

Command example:

The following output displays when you provide no optional argument:

```
(config)# show fip-snooping fcf
--------------------------------------------------------------------------------
Interface VLAN ENodes FPMA/ FC-MAP       FCF-MAC       Name-ID     Fabric-Name
                      SPMA
--------------------------------------------------------------------------------
1/0/11     1   2      FPMA 0e:fc:00 00:0d:ec:b2:2c:80 20:65:00:0d: 20:65:00:0d:
                                                     ec:b1:9e:81  ec:97:52:c1
3/0/10     1   1      FPMA 0e:fc:00 00:0d:ec:b2:2c:81 00000000     00000000
3/0/15    100  1      FPMA 0e:fc:10 00:0c:ab:2c:eb:12 00000000     00000000
```

Command example:

The following output displays when you provide the optional argument:

```
(NETGEAR Switch)# show  fip-snooping   fcf   00:0d:ec:b2:2c:81
Interface                      3/0/10
VLAN                           1
ENodes                         1
FPMA/SPMA                      FPMA
FCF-MAC                        00:0d:ec:b2:2c:81
```

```
FC-MAP                          0e:fc:00
Name-ID                         20:65:00:0d:ec:b1:9e:81
Fabric-Name                     20:65:00:0d:ec:97:52:c1
Sessions                        3
D-bit                           0
Available for Login             1
Priority                        2
FKA-ADV(FKA_ADV_PERIOD*5)       250
FCF Expiry Time                 219
Time Elapsed                    0 days, 2 hours, 8 minutes
```

show fip-snooping sessions

Use the **show fip-snooping sessions** command in User EXEC or Privileged EXEC mode to display information about the active FIP snooping sessions.

Note: This command can only be entered after FIP snooping is enabled using the **feature fip-snooping** command. Otherwise, it does not appear in the CLI syntax tree.

Format	show fip-snooping sessions [vlan *vlan-id* | interface *interface-id* | fcf *fcf-mac* [enode *enode-mac*]] [detail]
Mode	User EXEC Privileged EXEC

Parameter	Description
Interface-id	ID of an interface on which FIP snooping has been enabled.
FCF-MAC	MAC address of the FCF that is part of the session.
ENode-MAC	MAC address of the ENode that is part of the session.
VLAN	ID number of the VLAN that contains the session.
FCoE MAC	Source MAC address of the FCoE packets that are originated by the ENode as part of the session.
FC-ID	Fiber Channel ID of the virtual port that was created by the FCF when the ENode VN_Port did a FLOGI/NPIV/FDISC request.

The command output format is different when the **detail** option is used. The information below is displayed.

Parameter	Description
VLAN	VLAN to which the session belongs.
FC-MAP	FCMAP value used by the FCF.

Parameter	Description
FCFs	Number of FCFs discovered.
ENodes	Number of ENodes discovered.
Sessions	Total virtual sessions in FCoE VLAN.
FCF Information	
Interface	Interface on which the FCF is discovered.
MAC	MAC address of the FCF.
ENodes	Total number of ENodes that are connected to the FCF.
Sessions	Total number of virtual sessions accepted by FCF in the associated VLAN.
ENode Information	
Interface	Interface to which the ENode is connected.
MAC	MAC address of the ENode.
Sessions	Total number of virtual sessions originated from ENodes to FCF in the VLAN.
Waiting	Total number of virtual connections waiting for FCF acceptance in the VLAN.
Session Information	
FCoE-MAC	Source MAC address of the FCoE packets that are originated by the ENode as part of the session.
Request (FP, SP)	FIP session request type sent by ENode. This can be FLOGI or FDESC (NPIV FDISC). Whereas FP and SP values are the FP bit and the SP bit values in the FLOGI or NPIV FDISC request respectively.
Expiry Time	This is virtual connection/session expiry interval. This is used to monitor the status of the session. Session entry is removed when the value reaches 0. This value is reset to 450 secs (5*90 secs) every time an associated VN_Port FKA is received from the ENode. This is ignored (marked as **NA**) if the D-bit is set to one in the FCF Discovery Advertisements.
Mode	This is the addressing mode in use by the VN_Port at ENode. In other words, this is the type of MAC address granted (selected and returned) by FCF. This can be one of the addressing modes, i.e. FPMA or SPMA.
State	This is the state of the virtual session. The state is displayed as Tentative during the process of ENode login to FCF (using FLOGI or FDESC). It displays Active after ENode and FCF establish a successful virtual connection.
Session-Time	Time elapsed after this successful virtual session is established by ENode with FCF. The value is displayed in xd, yh, zm format where x represents number of days, y represents hours and z represents minutes elapsed following this successful virtual session. This field has no useful information for waiting sessions.

Command example:

The following output displays when you do not specify any arguments:

```
(NETGEAR Switch)# show fip-snooping sessions
--------------------------------------------------------------------------------
     FCF-MAC            ENode-MAC     VLAN      FCoE-MAC        FC-ID
--------------------------------------------------------------------------------
00:0d:ec:b2:2c:80  00:0c:29:65:82:bc  100   0e:fc:00:ad:00:00  38:0f:db
00:0d:ec:b2:2c:80  00:0c:29:65:82:bc  100   0e:fc:00:ad:00:01  38:0f:dc
00:0d:ec:b2:2c:80  00:0c:29:65:82:bc  100   0e:fc:00:ad:00:02  38:0f:dd
00:0d:ec:b2:2c:80  00:0c:29:65:82:bc  100   0e:fc:00:ad:00:05  38:0f:e1
00:0d:ec:b2:2c:80  00:0c:29:65:82:bc  100   0e:fc:00:ad:00:07  38:0f:e3
00:0d:ec:b2:2c:80  00:0c:29:65:82:bc  100   0e:fc:00:ad:00:10  38:0f:e6
00:0d:ec:b2:2c:80  00:0c:29:65:82:bc  100   0e:fc:00:ad:00:19  38:0f:ee
00:0e:ad:12:23:53  00:0d:29:12:22:a6  200   0e:fc:11:aa:bb:00  44:23:a4
00:0e:ad:12:23:53  00:0d:29:12:22:a6  200   0e:fc:11:aa:bb:01  44:02:ab
00:0e:ad:12:23:53  00:0d:29:23:14:22  200   0e:fc:11:aa:bb:02  44:35:1b
00:0e:ad:12:23:53  00:0d:29:23:14:22  200   0e:fc:11:aa:bb:03  44:35:2a
00:0e:ad:12:23:53  00:0d:29:23:14:22  200   0e:fc:11:aa:bb:04  44:36:3b
```

Command example:

The following output displays when you specify the detail option:

```
(NETGEAR Switch)# show fip-snooping sessions detail

VLAN: 100   FC-MAP: 0e:fc:00        FCFs:  1   ENodes: 1   Sessions: 7
   <FCF Information>
   Interface: 3/0/15   MAC: 00:0d:ec:b2:2c:80 ENodes: 1   Sessions: 7
      <ENode Information>
      Interface: 2/0/1    MAC: 00:0c:29:65:82:bc Sessions:  7   Waiting: 0
         <Session Information>
         FCoE-MAC           Request    Expiry  Mode State      Session-Time
                            (FP,SP)    Time
         0e:fc:00:ad:00:00  FLOGI(1,1) 200     FPMA ACTIVE     0d, 04h, 20m
         0e:fc:00:ad:00:01  FDESC(1,1) 259     FPMA ACTIVE     0d, 04h, 19m
         0e:fc:00:ad:00:02  FDESC(1,1) 215     FPMA ACTIVE     0d, 04h, 18m
         0e:fc:00:ad:00:05  FDESC(1,1) 231     FPMA ACTIVE     0d, 04h, 10m
         0e:fc:00:ad:00:07  FDESC(1,1) 189     FPMA ACTIVE     0d, 04h, 01m
         0e:fc:00:ad:00:10  FDESC(1,1) 210     FPMA ACTIVE     0d, 02h, 07m
         0e:fc:00:ad:00:19  FDESC(1,1) 222     FPMA ACTIVE     0d, 01h, 20m
--------------------------------------------------------------------------------
VLAN: 200   FC-MAP: 0e:fc:11        FCFs:  1   ENodes: 2   Sessions: 5

   <FCF Information>
   Interface: 3/0/11   MAC: 00:0e:ad:12:23:53 ENodes: 2   Sessions: 5

      <ENode Information>
```

```
   Interface: 1/0/10   MAC: 00:0d:29:12:22:a6 Sessions: 2    Waiting: 0
      <Session Information>
      FCoE-MAC          Request    Expiry  Mode State      Session-Time
                        (FP,SP)    Time
      0e:fc:11:ad:00:00 FLOGI(1,1) 242     FPMA ACTIVE     0d, 02h, 30m
      0e:fc:11:ad:00:01 FDESC(1,1) 245     FPMA ACTIVE     0d, 02h, 28m
   <ENode Information>
   Interface: 1/0/11   MAC: 00:0d:29:23:14:22 Sessions: 3    Waiting: 1
      <Session Information>
      FCoE-MAC          Request    Expiry  Mode State      Session-Time
                        (FP,SP)    Time
      0e:fc:11:ad:00:02 FLOGI(1,1) 202     FPMA ACTIVE     0d, 02h, 20m
      0e:fc:11:ad:00:03 FDESC(1,1) 228     FPMA ACTIVE     0d, 01h, 18m
      0e:fc:11:ad:00:03 FDESC(1,1) 232     FPMA ACTIVE     0d, 01h, 02m
      ----------------- FDESC(1,1) ---     FPMA TENTATIVE  ------------
```

Command example:

The following output displays sessions between the specified FCF and ENode:

```
(NETGEAR Switch)# show fip-snooping sessions fcf 00:0e:ad:12:23:53 enode
00:0d:29:12:22:a6
--------------------------------------------------------------------------------
     FCF-MAC            ENode-MAC     VLAN      FCoE-MAC       FC-ID
--------------------------------------------------------------------------------
00:0e:ad:12:23:53  00:0d:29:12:22:a6  200   0e:fc:11:aa:bb:00  44:23:a4
00:0e:ad:12:23:53  00:0d:29:12:22:a6  200   0e:fc:11:aa:bb:01  44:02:ab
```

Command example:

The following output displays sessions between the specified FCF and ENode with the detail option:

```
(NETGEAR Switch)# show fip-snooping sessions fcf 00:0e:ad:12:23:53 enode
00:0d:29:12:22:a6 detail

VLAN: 200   FC-MAP: 0e:fc:11        FCFs:  1   ENodes: 2   Sessions: 5

   <FCF Information>
   Interface: 3/0/11    MAC: 00:0e:ad:12:23:53 ENodes: 2   Sessions: 5

      <ENode Information>
      Interface: 1/0/10   MAC: 00:0d:29:12:22:a6 Sessions: 2    Waiting: 0
         <Session Information>
         FCoE-MAC          Request    Expiry  Mode State      Session-Time
                           (FP,SP)    Time
         0e:fc:11:ad:00:00 FLOGI(1,1) 242     FPMA ACTIVE     0d, 02h, 30m
         0e:fc:11:ad:00:01 FDESC(1,1) 245     FPMA ACTIVE     0d, 02h, 28m
```

show fip-snooping statistics

Use the **show fip-snooping statistics** command in User EXEC or Privileged EXEC mode to display the statistics of the FIP packets snooped in the VLAN or on an interface. If the optional (VLAN or interface) argument is not given, this command displays the statistics for all of the FIP snooping enabled VLANs.

Note: This command can only be entered after FIP snooping is enabled using the **feature fip-snooping** command. Otherwise, it does not appear in the CLI syntax tree.

Format	`show fip-snooping statistics [vlan vlan-id] | [interface interface-id]`
Mode	User EXEC Privileged EXEC

Parameter	Description
vlan-id	A VLAN on which FIP snooping is enabled.
interface-id	An interface belonging to a VLAN on which FIP snooping is enabled.

The following table describes the packet counters per FIP Operation.

Packet Counter	Description
VR	Number of VLAN Request messages received on the VLAN.
VN	Number of VLAN Notification messages received on the VLAN.
MDS	Number of Multicast Discovery Solicitation messages snooped on the VLAN.
UDS	Number of Unicast Discovery Solicitation messages snooped on the VLAN.
FLOGI	Number of Fabric Logins snooped on the VLAN.
FDISC	Number of fabric discovery logins snooped on the VLAN.
LOGO	Number of Fabric Logouts on the VLAN.
VNPort-keep-alive	Number of VN_Port keepalive messages snooped on the VLAN.
MDA	Number of Multicast Discovery Advertisement messages snooped on the VLAN.
UDA	Number of Unicast Discovery Advertisement messages snooped on the VLAN.
FLOGI_ACC	Number of Fabric Logins accepted on the VLAN.
FLOGI_RJT	Number of Fabric Logins rejected on the VLAN.
FDISC_ACC	Number of Fabric Discoveries accepted on the VLAN.
FDISC_RJT	Number of Fabric Discoveries rejected on the VLAN.

Packet Counter	Description
LOGO_ACC	Number of Fabric Logouts accepted on the VLAN.
LOGO_RJT	Number of Fabric Logouts rejected on the VLAN.
CVL	Number of Clear Virtual Links actions on the VLAN.

The following table describes the other interface or session-related counters.

Other Counters	Description
Number of Virtual Session Timeouts	Number of Virtual sessions removed due to session timer expiry.
Number of FCF Session Timeouts	Number of ACTIVE sessions timed out due to Discovery Advertisements expiry from FCFs in the VLAN.
Number of Session configuration failures	Number of sessions in the VLAN that failed to be configured in the hardware.
Number of Sessions denied with FCF limit	Number of sessions that are denied to be created for the new FCF as the number of FCFs reached the maximum allowed in the VLAN.
Number of Sessions denied with ENode limit	Number of session create requests that are denied for the new ENode as the number of ENodes reached the maximum allowed in the system.
Number of Sessions denied with System limit	Number of sessions that are denied to be created as the number of sessions reached the maximum allowed in the system.

When an interface is provided as an argument, interface applicable statistics are only displayed. See the third example for applicable statistics on an interface.

Command example:

The following output displays when you specify no optional arguments supplied:

```
(NETGEAR Switch)# show fip-snooping statistics
VLAN: 4
---------------------------------
FIP-Operation    Number of Pkts
VR                2
VN                2
MDS               2
UDS               2
FLOGI             2
FDISC             2
LOGO              0
VNPort-keep-alive 200
MDA               25
```

```
UDA               2
FLOGI_ACC         2
FLOGI_RJT         0
FDISC_ACC         2
FDISC_RJT         0
LOGO_ACC          0
LOGO_RJT          0
CVL               0
---------------------------------
Number of Virtual Session Timeouts:23
Number of FCF Session Timeouts:    6
Number of Session configuration failures: 10
Number of Sessions denied with FCF limit:  10
Number of Sessions denied with ENode limit:  10
Number of Sessions denied with System limit:   12

VLAN: 200
-------------------------------
FIP-Operation    Number of Pkts
VR                2
VN                2
MDS               5
UDS               4
FLOGI             5
FDISC             5
LOGO              1
VNPort-keep-alive 310
MDA               35
UDA               3
FLOGI_ACC         4
FLOGI_RJT         0
FDISC_ACC         15
FDISC_RJT         0
LOGO_ACC          1
LOGO_RJT          0
CVL               0
-------------------------------

Number of Virtual Session Timeouts:2
Number of FCF Session Timeouts:    0
Number of Session configuration failures: 10
Number of Sessions denied with FCF limit:  0
Number of Sessions denied with ENode limit:  0
Number of Sessions denied with System limit:   21
```

Command example:

The following output displays when you specify an optional VLAN argument:

```
(NETGEAR Switch)# show fip-snooping statistics vlan 200

VLAN: 200

-------------------------------
FIP-Operation    Number of Pkts
-------------------------------
VR               2
VN               2
MDS              5
UDS              4
FLOGI            5
FDISC            5
LOGO             1
VNPort-keep-alive 310
MDA              35
UDA              3
FLOGI_ACC        4
FLOGI_RJT        0
FDISC_ACC        15
FDISC_RJT        0
LOGO_ACC         1
LOGO_RJT         0
CVL              0
-------------------------------

Number of Virtual Session Timeouts:2
Number of FCF Session Timeouts:    0
Number of Session configuration failures: 10
Number of Sessions denied with FCF limit:  0
Number of Sessions denied with ENode limit:  0
Number of Sessions denied with System limit:   21
```

Command example:

The following output displays when you specify the optional interface argument:

```
(NETGEAR Switch)# show fip-snooping statistics interface 1/0/5

-------------------------------
FIP-Operation    Number of Pkts
-------------------------------
VR               2
VN               2
```

```
MDS                5
UDS                1
FLOGI              2
FDISC              5
LOGO               1
VNPort-keep-alive 310
MDA                35
UDA                3
FLOGI_ACC          4
FLOGI_RJT          0
FDISC_ACC          15
FDISC_RJT          0
LOGO_ACC           1
LOGO_RJT           0
CVL                0
--------------------------------

Number of Virtual Session Timeouts:2
Number of FCF Session Timeouts:    0
Number of Session configuration failures: 10
Number of Sessions denied with FCF limit:  0
Number of Sessions denied with ENode limit:  0
Number of Sessions denied with System limit:   21
```

show fip-snooping vlan

Use the **show fip-snooping vlan** command in User EXEC or Privileged EXEC mode to display the FCoE VLANs information and, additionally, the FIP snooping port status when optional argument is specified.

Note: This command can only be entered after FIP snooping is enabled using the **feature fip-snooping** command. Otherwise, it does not appear in the CLI syntax tree.

Format	`show fip-snooping vlan [vlan-id]`
Mode	User EXEC Privileged EXEC

Parameter	Description
vlan-id	A VLAN enabled for FIP snooping.
VLAN	VLAN in which FIP snooping is enabled/operational.
FC-MAP	FCoE mapped address prefix of the FCoE forwarder for the FCoE VLAN.

Parameter	Description
FCFs	Number of FCFs discovered.
ENodes	Number of ENodes discovered.
Sessions	Total virtual sessions in FCoE VLAN.

Command example:

```
(NETGEAR Switch)# show fip-snooping

Global Mode:        Enable
FCoE VLAN List :   2,4,5-8
FCFs:                    2
ENodes:                  2
Sessions:               10
Max VLANs:               8
Max FCFs in VLAN:        4
Max ENodes:            312
Max Sessions:         1024
```

clear fip-snooping statistics

Use the **`clear fip-snooping statistics`** command in User EXEC or Privileged EXEC mode to clear the FIP Snooping statistics in the supplied VLAN or on a supplied interface. If the optional (VLAN or interface) argument is not given, this command clears the statistics on all FIP snooping-enabled VLANs.

Note: This command can only be entered after FIP snooping is enabled using the **`feature fip-snooping`** command. Otherwise, it does not appear in the CLI syntax tree.

Format	`clear fip-snooping statistics [vlan` *`vlan-id`*`] | [interface` *`interface-id`*`]`
Mode	User EXEC Privileged EXEC

Parameter	Description
vlan-id	A VLAN on which FIP snooping is enabled.
interface-id	An interface belonging to a VLAN on which FIP snooping is enabled.

Priority-Based Flow Control Commands

Ordinarily, when flow control is enabled on a physical link, it applies to all traffic on the link. When congestion occurs, the hardware sends pause frames that temporarily suspend traffic flow. Pausing traffic helps prevent buffer overflow and dropped frames.

Priority-based flow control (PFC) provides a way to distinguish which traffic on physical link is paused when congestion occurs, based on the priority of the traffic. An interface can be configured to pause only high priority (i.e., loss-sensitive) traffic when necessary prevent dropped frames, while allowing traffic that has greater loss tolerance to continue to flow on the interface.

Priorities are differentiated by the priority field of the IEEE 802.1Q VLAN header, which identifies an IEEE 802.1p priority value. In NETGEAR Managed Switch, these priority values must be mapped to internal class-of-service (CoS) values.

To enable priority-based flow control for a particular CoS value on an interface:

1. Ensure that VLAN tagging is enabled on the interface so that the 802.1p priority values are carried through the network (see *Provisioning (IEEE 802.1p) Commands* on page 422).
2. Ensure that 802.1p priority values are mapped to NETGEAR Managed Switch CoS values (see *classofservice dot1p-mapping* on page 1035).

When priority-flow-control is disabled, the interface defaults to the IEEE 802.3x flow control setting for the interface. When priority-based flow control is enabled, the interface will not pause any CoS unless there is at least one no-drop priority.

priority-flow-control mode

Use the **`priority-flow-control mode on`** command in Datacenter-Bridging Config mode to enable Priority-Flow-Control (PFC) on the given interface.

PFC must be enabled before FIP snooping can operate over the interface. Use the **no** form of the command to return the mode to the default (off). VLAN tagging (trunk or general mode) must be enabled on the interface in order to carry the dot1p value through the network. Additionally, the dot1mapping to class-of-service must be set to one-to-one.

When PFC is enabled on an interface, the normal PAUSE control mechanism is operationally disabled.

Default	Priority-flow-control mode is off (disabled) by default.
Format	`priority-flow-control mode {on | off}`
Mode	Datacenter-Bridging Config mode

Parameter	Description
on	Enable PFC on the interface.
off	Disable PFC on the interface.

Command example:

The following example enables PFC on an interface:

```
s1(config)#interface te1/0/1
s1(config-if-Te1/0/1)#datacenter-bridging
s1(config-if-dcb)#priority-flow-control mode on
```

no priority-flow-control mode

Use the **no priority-flow-control mode** command to return the PFC mode to the default (off).

Format	no priority-flow-control mode
Mode	Datacenter-Bridging Config mode

priority-flow-control priority

Use the **priority-flow-control priority** command in Datacenter-Bridging Config mode to enable the priority group for lossless (no-drop) or lossy (drop) behavior on the selected interface. Up to two lossless priorities can be enabled on an interface. The administrator must configure the same no-drop priorities across the network in order to ensure end-to-end lossless behavior.

The command has no effect on interfaces not enabled for PFC. VLAN tagging needs to be turned on in order to carry the dot1p value through the network. Additionally, the dot1pmapping to class of service must be set to one to one.

Default	The default behavior for all priorities is drop.
Format	priority-flow-control priority priority-list {drop | no-drop}
Mode	Datacenter-Bridging Config mode

Parameter	Description
drop	Disable lossless behavior on the selected priorities.
no-drop	Enable lossless behavior on the selected priorities.

Command example:

The following example sets priority 3 to no drop behavior:

```
s1(config)#interface te1/0/1
s1(config-if-Te1/0/1)#datacenter-bridging
s1(config-if-dcb)#priority-flow-control mode on
s1(config-if-dcb)#priority-flow-control priority 1 no-drop
```

no priority-flow-control priority

Use the **no priority-flow-control priority** command in Datacenter-Bridging Config mode to enable lossy behavior on all priorities on the interface. This has no effect on interfaces not enabled for PFC or with no lossless priorities configured.

Format	`no priority-flow-control priority`
Mode	Datacenter-Bridging Config mode

clear priority-flow-control statistics

Use the **clear priority-flow-control statistics** command to clear all global and interface PFC statistics.

Format	`clear priority-flow-control statistics`
Mode	Privileged EXEC

Command example:

```
console#clear priority-flow-control statistics
```

show interface priority-flow-control

Use the **show interface priority-flow-control** command in Privileged EXEC mode to display the PFC information of a given interface or all interfaces.

Format	`show interface [`*`unit/slot/port`*`] priority-flow-control`
Mode	Privileged EXEC

Parameter	Description
unit/slot/port	A valid Ethernet port.

When an interface number is not provided, the following information displays for all interfaces.

Parameter	Description
Interface Detail	The port for which data is displayed.
PFC Operational Status	The operational status of the interface.
PFC Configured State	The administrative mode of PFC on the interface.
Configured Drop Priorities	The 802.1p priority values that are configured with a drop priority on the interface. Drop priorities do not participate in pause.
Configured No-Drop Priorities	The 802.1p priority values that are configured with a no-drop priority on the interface. If an 802.1p priority that is designated as no-drop is congested, the priority is paused.

Parameter	Description
Operational Drop Priorities	The 802.1p priority values that the switch is using with a drop priority. The operational drop priorities might not be the same as the configured priorities if the interface has accepted different priorities from a peer device
Configured No-Drop Priorities	The 802.1p priority values that the switch is using with a no-drop priority. The operational drop priorities might not be the same as the configured priorities if the interface has accepted different priorities from a peer device
Delay Allowance	The operational status of the interface.
Peer Configuration Compatible	Indicates whether the local switch has accepted a compatible configuration from a peer switch.
Compatible Configuration Count	The number of received configurations accepted and processed as valid. This number does not include duplicate configurations.
Incompatible Configuration Count	The number of received configurations that were not accepted from a peer device because they were incompatible.
Priority	The 802.1p priority value.
Received PFC Frames	The number of PFC frames received by the interface with the associated 802.1p priority.
Transmitted PFC Frames	The number of PFC frames transmitted by the interface with the associated 802.1p priority.

Command example:

```
(NETGEAR Switch) #show interface 0/1 priority-flow-control

Interface Detail:                  0/1
PFC Configured State:              Disabled
PFC Operational State:             Enabled
Configured Drop Priorities:        2-7
Operational Drop Priorities:       2-7
Configured No-Drop Priorities:     0-1
Operational No-Drop Priorities:    0-1
Delay Allowance:                   32456 bit times
Peer Configuration Compatible:     True
Compatible Configuration Count:    3
Incompatible Configuration Count:  1

Priority  Received PFC Frames     Transmitted PFC Frames
--------  --------------------     ----------------------
00                       0
10                       0
20                       0
30                       0
40                       0
50                       0
60                       0
70                       0
```

Command example:

```
(NETGEAR Switch) #show interface priority-flow-control

Port      Drop          No-Drop       Oper
        Priorities    Priorities      State
------  ----------    ----------     -------
1/0/1    1-4,75,6                   Enabled
1/0/2    1-4,6-75                   Enabled
1/0/48   1-4,75,6                   Enabled
```

Routing Commands

10

This chapter describes the routing commands available in the NETGEAR Managed Switch CLI. The chapter contains the following sections:

- *Address Resolution Protocol Commands*
- *IP Routing Commands*
- *Router Discovery Protocol Commands*
- *Virtual LAN Routing Commands*
- *Virtual Router Redundancy Protocol Commands*
- *DHCP and BootP Relay Commands*
- *IP Helper Commands*
- *Open Shortest Path First Commands*
- *Routing Information Protocol Commands*
- *ICMP Throttling Commands*

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

- **Show commands**. Display switch settings, statistics, and other information.
- **Configuration command**s. 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

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.

Format	`arp` *`ipaddress macaddr`*
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.

Format	`no arp` *`ipaddress macaddr`*
Mode	Global Config

ip proxy-arp

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	`ip proxy-arp`
Mode	Interface Config

no ip proxy-arp

This command disables proxy ARP on a router interface.

Format	`no ip proxy-arp`
Mode	Interface Config

ip local-proxy-arp

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	`ip local-proxy-arp`
Mode	Interface Config

no ip local-proxy-arp

This command resets the local proxy ARP mode on the interface to the default value.

Format	`no ip local-proxy-arp`
Mode	Interface Config

arp cachesize

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	`arp cachesize` *`platform-specific-integer-value`*
Mode	Global Config

no arp cachesize

This command configures the default ARP cache size.

Format	`no arp cachesize`
Mode	Global Config

arp dynamicrenew

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 router 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	Privileged EXEC

no arp dynamicrenew

This command prevents dynamic ARP entries from renewing when they age out.

Format	`no arp dynamicrenew`
Mode	Privileged EXEC

arp purge

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.

Format	`arp purge` *`ipaddr`*
Mode	Privileged EXEC

arp resptime

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` *`seconds`*
Mode	Global Config

no arp resptime

This command configures the default ARP request response timeout.

Format	`no arp resptime`
Mode	Global Config

arp retries

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` *`retries`*
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

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` *`seconds`*
Mode	Global Config

no arp timeout

This command configures the default ARP entry ageout time.

Format	`no arp timeout`
Mode	Global Config

clear arp-cache

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 [gateway]`
Mode	Privileged EXEC

clear arp-switch

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

This command displays the Address Resolution Protocol (ARP) cache. The displayed results are not the total ARP entries. To view the total ARP entries, the 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 *unit/slot/port* 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

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 *unit/slot/port* 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.

routing

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

This command enables the IP Router Admin Mode for the supervisor blade.

Format	ip routing
Mode	Global Config

no ip routing

This command disables the IP Router Admin Mode for the supervisor blade.

Format	`no ip routing`
Mode	Global Config

ip address

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 676.

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 NETGEAR Managed Switch acts as a host, not a router, on these management interfaces.

Format	`ip address` *`ipaddr`* `{`*`subnetmask`* `|` */masklen*`} [secondary]`
Mode	Interface Config

Parameter	Description
ipaddr	The IP address of the interface.
subnetmask	A 4-digit dotted-decimal number which represents the subnet mask of the interface.
masklen	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	no ip address [*ipaddr subnetmask* [secondary]]
Mode	Interface Config

ip address dhcp

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

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` *ipaddr*
Mode	Interface Config

release dhcp

Use this command to force the DHCPv4 client to release the leased address from the specified interface. 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.

Format	`release dhcp` *`unit/slot/port`*
Mode	Privileged EXEC

renew dhcp

Use this command to force the DHCPv4 client to immediately renew an IPv4 address lease on the specified interface.

Note: This command can be used on in-band ports as well as the service or network (out-of-band) port.

Format	`renew dhcp` *`unit/slot/port`*
Mode	Privileged EXEC

renew dhcp network-port

Use this command to renew an IP address on a network port.

Format	`renew dhcp network-port`
Mode	Privileged EXEC

renew dhcp service-port

Use this command to renew an IP address on a service port.

Format	`renew dhcp service-port`
Mode	Privileged EXEC

ip route

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 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.

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	`ip route ipaddr subnetmask [nexthopip | Null0] [preference]`
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.

Format	`no ip route ipaddr subnetmask [nexthopip | Null0] [preference]`
Mode	Global Config

ip route default

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.

Default	preference—1
Format	`ip route default nexthopip [preference]`
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	`no ip route default [nexthopip] [preference]`
Mode	Global Config

ip route distance

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	`ip route distance` *number*
Mode	Global Config

no ip route distance

This command sets the default static route preference value in the router. Lower route preference values are preferred when determining the best route.

Format	`no ip route distance`
Mode	Global Config

ip netdirbcast

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 mtu

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 (unless OSPF has been instructed to ignore differences in IP MTU with the **ip ospf mtu-ignore** command.)

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 358) must take into account the size of the Ethernet header.

Default	1500 bytes
Format	`ip mtu` *size*
Mode	Interface Config

no ip mtu

This command resets the ip mtu to the default value.

Format	`no ip mtu`
Mode	Interface Config

encapsulation

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

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.

Format	`show dhcp lease [interface` *unit/slot/port*`]`
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.
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

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 interface

This command displays all pertinent information about the IP interface. 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 directly instead of in a *unit/slot/port* format.

The *vlan-id* is a number in the range 1–4093. The loopback *number* is in the range 0–7.

Format	show ip interface {*unit/slot/port* | vlan *vland-id* | loopback *number*}
Modes	Privileged EXEC User EXEC

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 *ip helper-address (Interface Config)* on page 736.
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.

Term	Definition
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..... 0NETGEAR-0010.1882.160E-vl10
```

show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router, and indicates how each IP address was assigned.

Format	`show ip interface brief`
Modes	Privileged EXEC User EXEC

Term	Definition
Interface	Valid slot 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 protocols

This command lists a summary of the configuration and status for each unicast routing protocol. The command lists routing protocols which are configured and enabled. If a protocol is selected on the command line, the display will be limited to that protocol.

Format	`show ip protocols [bgp | ospf | rip]`
Mode	Privileged Exec

Parameter	Description
BGP Section:	
Routing Protocol	BGP.
Router ID	The router ID configured for BGP.
Local AS Number	The AS number that the local router is in.
BGP Admin Mode	Whether BGP is globally enabled or disabled.
Maximum Paths	The maximum number of next hops in an internal or external BGP route.
Always Compare MED	Whether BGP is configured to compare the MEDs for routes received from peers in different ASs.
Maximum AS Path Length	Limit on the length of AS paths that BGP accepts from its neighbors.
Fast Internal Failover	Whether BGP immediately brings down an iBGP adjacency if the routing table manager reports that the peer address is no longer reachable.
Fast External Failover	Whether BGP immediately brings down an eBGP adjacency if the link to the neighbor goes down.
Distance	The default administrative distance (or route preference) for external, internal, and locally-originated BGP routes. The table that follows lists ranges of neighbor addresses that have been configured to override the default distance with a neighbor-specific distance. If a neighbor's address falls within one of these ranges, routes from that neighbor are assigned the configured distance. If a prefix list is configured, then the distance is only assigned to prefixes from the neighbor that are permitted by the prefix list.
Redistribution	A table showing information for each source protocol (connected, static, rip, and ospf). For each of these sources the distribution list and route-map are shown, as well as the configured metric. Fields which are not configured are left blank. For ospf, an additional line shows the configured ospf match parameters.

Parameter	Description
Prefix List In	The global prefix list used to filter inbound routes from all neighbors.
Prefix List Out	The global prefix list used to filter outbound routes to all neighbors.
Networks Originated	The set of networks originated through a network command. Those networks that are actually advertised to neighbors are marked “active.”
Neighbors	A list of configured neighbors and the inbound and outbound policies configured for each.
OSPFv2 Section:	
Routing Protocol	OSPFv2.
Router ID	The router ID configured for OSPFv2.
OSPF Admin Mode	Whether OSPF is enabled or disabled globally.
Maximum Paths	The maximum number of next hops in an OSPF route.
Routing for Networks	The address ranges configured with an OSPF network command.
Distance	The administrative distance (or “route preference”) for intra-area, inter-area, and external routes.
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.
Metric	The metric configured to be advertised with the default route.
Metric Type	The metric type for the default route.
Redist Source	A type of routes that OSPF is redistributing.
Metric	The metric to advertise for redistributed routes of this type.
Metric Type	The metric type to advertise for redistributed routes of this type.
Subnets	Whether OSPF redistributes subnets of classful addresses, or only classful prefixes.
Dist List	A distribute list used to filter routes of this type. Only routes that pass the distribute list are redistributed.
Number of Active Areas	The number of OSPF areas with at least one interface running on this router. Also broken down by area type.
ABR Status	Whether the router is currently an area border router. A router is an area border router if it has interfaces that are up in more than one area.
ASBR Status	Whether the router is an autonomous system boundary router. The router is an ASBR if it is redistributing any routes or originating a default route.
RIP Section	
RIP Admin Mode	Whether RIP is globally enabled.
Split Horizon Mode	Whether RIP advertises routes on the interface where they were received.

Parameter	Description
Default Metric	The metric assigned to redistributed routes.
Default Route Advertise	Whether this router is originating a default route.
Distance	The administrative distance for RIP routes.
Redistribution	A table showing information for each source protocol (connected, static, bgp, and ospf). For each of these source the distribution list and metric are shown. Fields which are not configured are left blank. For ospf, configured ospf match parameters are also shown.
Interface	The interfaces where RIP is enabled and the version sent and accepted on each interface.

Command example:

```
(NETGEAR Switch) #show ip protocols

Routing Protocol.......................... BGP
Router ID................................. 6.6.6.6
Local AS Number........................... 65001
BGP Admin Mode............................ Enable
Maximum Paths............................. Internal 32, External 32
Always compare MED ....................... FALSE
Maximum AS Path Length ................... 75
Fast Internal Failover ....................... Enable
Fast External Failover ....................... Enable

Distance.................................. Ext 20 Int 200 Local 200
  Address         Wildcard        Distance    Pfx List
  -------         --------        --------    --------
  172.20.0.0      0.0.255.255           40        None
  172.21.0.0      0.0.255.255           45           1

Prefix List In............................ PfxList1
Prefix List Out........................... None

Redistributing:
Source        Metric  Dist List               Route Map
--------- ----------  ---------------------- --------------------------
connected             connected_list
static         32120                         static_routemap
rip            30000                         rip_routemap
ospf                                         ospf_map
  ospf match: int ext1 nssa-ext2


   Networks Originated:
     10.1.1.0 255.255.255.0 (active)
```

```
     20.1.1.0 255.255.255.0

Neighbors:
172.20.1.100
   Filter List In..................... 1
   Filter List Out.................... 2
   Prefix List In..................... PfxList2
   Prefix List Out.................... PfxList3
   Route Map In....................... rmapUp
   Route Map Out...................... rmapDown
172.20.5.1
   Prefix List Out.................... PfxList12


Routing Protocol..................... OSPFv2
Router ID............................ 6.6.6.6
OSPF Admin Mode...................... Enable
Maximum Paths........................ 32
Routing for Networks................. 172.24.0.0 0.0.255.255 area 0
                                      10.0.0.0 0.255.255.255 area 1
                                      192.168.75.0 0.0.0.255 area 2
Distance............................. Intra 110 Inter 110 Ext 110

Default Route Advertise.............. Disabled
Always............................... FALSE
Metric............................... Not configured
Metric Type.......................... External Type 2

Redist
Source      Metric       Metric Type     Subnets    Dist List
---------  -------       -----------     -------    ---------
static     default                2         Yes         None
connected       10                2         Yes            1

Number of Active Areas............... 3 (3 normal, 0 stub, 0 nssa)
ABR Status........................... Yes
ASBR Status.......................... Yes


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
ospf                     20 int ext1 ext2 nssa-ext1

Interface              Send        Recv
---------              ----        ----
0/25                   RIPv2       RIPv2
```

show ip route

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 given *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**, **ospf**, **rip**, **static**, or **bgp**. Use the **all** parameter to display all routes including best and nonbest 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 nonbest 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	show ip route [{*ip-address* [*protocol*] | {*ip-address mask* [longer-prefixes] [*protocol*] | *protocol*} [all] | all}]
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.
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 router, you can configure a static reject route on the router. 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. The reject route added in the RTO is of the type OSPF Inter-Area. Reject routes (routes of REJECT type installed by any protocol) are not redistributed by OSPF/RIP. Reject routes are supported in both OSPFv2 and OSPFv3.

Command example:

```
(NETGEAR Routing) #show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2

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
OIA 10.10.10.0/24 [110/6] via 5.5.5.2,   00h:00m:01s,  0/5
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
```

Command example:

The following output indicates a truncated route:

```
(NETGEAR Switch) #show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2

O E1   100.1.161.0/24 [110/10] via 172.20.11.100,   00h:00m:13s,  2/11 T
O E1   100.1.162.0/24 [110/10] via 172.20.11.100,   00h:00m:13s,  2/11 T
O E1   100.1.163.0/24 [110/10] via 172.20.11.100,   00h:00m:13s,  2/11 T
```

show ip route ecmp-groups

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 summary

This command displays a summary of the state of the routing table. When the optional `all` keyword is given, 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	`show ip route summary [all]`
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.
BGP Routes	Total number of routes installed by the BGP protocol.
External	The number of external BGP routes.
Internal	The number of internal BGP routes.
Local	The number of local BGP routes.
OSPF Routes	Total number of routes installed by OSPF protocol.
Intra Area Routes	Total number of Intra Area routes installed by OSPF protocol.
Inter Area Routes	Total number of Inter Area routes installed by OSPF protocol.
External Type-1 Routes	Total number of External Type-1 routes installed by OSPF protocol.
External Type-2 Routes	Total number of External Type-2 routes installed by OSPF protocol.
Reject Routes	Total number of reject routes installed by all protocols.

Term	Definition
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. 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.
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
BGP Routes.................................... 10
  External.................................... 0
  Internal.................................... 10
  Local....................................... 0
OSPF Routes................................... 1004
  Intra Area Routes........................... 4
  Inter Area Routes........................... 1000
  External Type-1 Routes...................... 0
  External Type-2 Routes...................... 0
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

This command lets you reset the IPv4 routing table counters or remove various types of routes in the IPv4 routing table.

Format	`clear ip route {all | bgp [`*`ip-address subnet-mask`*` [interface `*`unit/slot/port`*`]] | counters | ospf [`*`ip-address subnet-mask`*` [interface `*`unit/slot/port`*`] | rip [`*`ip-address subnet-mask`*` [interface `*`unit/slot/port`*`]]}`
Mode	Privileged EXEC

Term	Definition
all	Removes all dynamic routes from the IPv4 routing table. Static routes are not removed.
bgp	Removes all BGP routes from the IPv4 routing table. By using the *`ip-address`* and *`subnet-mask`* parameters you can remove specific BGP routes. In addition, you can remove specific BGP routes from specific next hop interfaces by using the **`interface`** option and *`unit/slot/port`* parameter.
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 686). 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.
ospf	Removes all OSPF routes from the IPv4 routing table. By using the *`ip-address`* and *`subnet-mask`* 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 *`unit/slot/port`* parameter.
rip	Removes all RIP routes from the IPv4 routing table. By using the *`ip-address`* and *`subnet-mask`* 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 *`unit/slot/port`* parameter.

show ip route preferences

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.
BGP External	The BGP external route preference value.
OSPF Intra	The OSPF Intra route preference value.

Term	Definition
OSPF Inter	The OSPF Inter route preference value.
OSPF External	The OSPF External route preference value.
RIP	The RIP route preference value.
Internal BGP	The BGP internal route preference value.
Local BGP	The BGP local 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
OSPF Intra................................ 110
OSPF Inter................................ 110
OSPF External............................. 110
RIP....................................... 120
Configured Default Gateway................ 253
DHCP Default Gateway...................... 254
```

show ip stats

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

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

Note: Routing policy commands are supported on M6100 series switches only.

ip policy route-map

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	`ip policy route-map-name`
Mode	Interface Config

Command example:

```
(NETGEAR Routing) (Config)#interface 1/0/1
(NETGEAR Routing) (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	`no ip policy route-map-name`
Mode	Interface Config

ip prefix-list

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 of a sequence of prefix list entries ordered by their sequence numbers. A router 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 assume if a given prefix does not match any entries of a prefix list. Once a match or deny occurs the router does not go through the rest of the list. A prefix list may be used within a route map to match a route's prefix using the command *match ip address* on page 698.

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 list-name [seq number] {{permit | deny} network/length [ge length] [le length] | renumber renumber-interval first-statement-number}`
Mode	Global Configuration

Parameter	Description
list-name	The text name of the prefix list. Up to 32 characters.
seq number	(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 ranges 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.
network/length	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.
ge length	(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.
le length	(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.
renumber	(Optional) Provides the option to renumber the sequence numbers of the IP prefix list statements with a given interval starting from a particular sequence number. The valid range for *renumber-interval* is 1–100, and the valid range for *first-statement-number* 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

To delete a prefix list or a statement in a prefix list, use the **no** form of this command. The command **no ip prefix-list list-name** 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` *`list-name`* `[seq` *`number`*`] {permit | deny}` *`network/length`* `[ge` *`length`*`] [le` *`length`*`]`
Mode	Global Configuration

ip prefix-list description

To apply a text description to a prefix list, use the **ip prefix-list description** command in Global Configuration mode.

Default	No description is configured by default.
Format	`ip prefix-list` *`list-name`* `description` *`text`*
Mode	Global Configuration

Parameter	Description
list-name	The text name of the prefix list.
description text	Text description of the prefix list. Up to 80 characters.

no ip prefix-list description

To remove the text description, use the **no ip prefix-list description** command.

Format	`no ip prefix-list` *`list-name`* `description`
Mode	Global Configuration

ipv6 prefix-list (routing policy commands)

Use this command to create IPv6 prefix lists. An IPv6 prefix list can contain only ipv6 addresses. Prefix lists allow matching of route prefixes with those specified in the prefix list. Each prefix list includes of a sequence of prefix list entries ordered by their sequence numbers. A router sequentially examines each prefix list entry to determine if the route's prefix matches that of the entry. For IPv6 routes, only IPv6 prefix lists are matched. An empty or nonexistent prefix list permits all prefixes. An implicit deny is assumed if a given prefix does not match any entries of a prefix list. Once a match or deny occurs the router does not go through the rest of the list. An IPv6 prefix list may be used within a route map to match a route's prefix using the **match ipv6 address** command. A route map may contain both IPv4 and IPv4 prefix lists. If a route being matched is an IPv6 route, only the IPv6 prefix lists are matched.

Up to 128 prefix lists may be configured. The maximum number of statements allowed in prefix list is 64. These numbers indicate only IPv6 prefix lists. IPv4 prefix lists may be configured in appropriate numbers independently.

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	`ipv6 prefix-list` *`list-name`* `[seq` *`number`*`] {{permit | deny}` *`ipv6-prefix/prefix-length`* `[ge` *`length`*`] [le` *`length`*`] | description` *`text`* `| renumber` *`renumber-interval first-statement-number`*`}`
Mode	Global Configuration

Parameter	Description
list-name	The text name of the prefix list. Up to 32 characters.
seq number	(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 ranges 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.
ipv6-prefix/prefix-length	Specifies the match criteria for routes being compared to the prefix list statement. The ipv6-prefix can be any valid IPv6 prefix where the address is specified in hexadecimal using 16-bit values between colons. The prefix-length is the The length of the IPv6 prefix, given as a decimal value that indicates 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 decimal value.
ge length	(Optional) If this option is configured, specifies a prefix length greater than or equal to the ipv6-prefix/prefix-length. It is the lowest value of a range of the length.
le length	(Optional) If this option is configured, specifies a prefix length less than or equal to the ipv6-prefix/prefix-length. It is the highest value of a range of the length.
Description	A description of the prefix list. It can be up to 80 characters in length.
renumber	(Optional) Provides the option to renumber the sequence numbers of the IPv6 prefix list statements with a given interval starting from a particular sequence number.

Command example:

The following example configures a prefix list that allows routes with one of two specific destination prefixes, 2001::/64 and 5F00::/48:

```
(R1)(config)# ipv6 prefix-list apple seq 10 permit 2001::/64
(R1)(config)# ipv6 prefix-list apple seq 20 permit 5F00::/48
```

no ipv6 prefix-list

Use this command to deletes either the entire prefix list or an individual statement from a prefix list.

Format	`no ipv6 prefix-list` *`list-name`*
Mode	Global Configuration

Note: The description must be removed using **`no ip prefix-list description`** command (see *no ip prefix-list description* on page 694) before using this command to delete an IPv6 Prefix List.

route-map

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. NETGEAR Managed Switch accepts up to 64 route maps.

Default	No route maps are configured by default. If no permit or deny tag is given, **`permit`** is the default.
Format	`route-map` *`map-tag`* `[permit | deny] [`*`sequence-number`*`]`
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
```

```
(NETGEAR Switch)(config) router bgp 1
(NETGEAR Switch)(Config-router) redistribute ospf route-map redist-rm
```

no route-map

To delete a route map or one of its statements, use the **no route-map** command.

Format	no route-map *map-tag* [permit | deny] [*sequence-number*]
Mode	Global Configuration

match as-path

The **match as-path** command matches BGP autonomous system paths against an AS path access list. If you enter a new match as-path term in a route map statement that already has a match as-path term, the AS path list numbers in the new term are added to the existing match term, up to the maximum number of lists in a term. A route is considered a match if it matches any one or more of the AS path access lists the match term refers to.

Format	match as-path *as-path-list-number*
Mode	Route Map Configuration

Parameter	Description
as-path-list-number	An integer from 1 to 500 identifying the AS path access list to use as match criteria.

no match as-path

This command deletes the match as-path term that matches BGP autonomous system paths against an AS path access list.

Format	no match as-path *as-path-list-number*
Mode	Route Map Configuration

match community

To configure a route map to match based on a BGP community list, use the **match community** command in Route Map Configuration mode. If the community list returns a permit action, the route is considered a match. If the match statement refers to a community list that is not configured, no routes are considered to match the statement.

Format	match community *community-list* [*community-list...*] [exact-match]
Mode	Route Map Configuration

Parameter	Description
community-list	The name of a standard community list. Up to eight names can be included in a single match term.
exact-match	(Optional) When this option is given, a route is only considered a match if the set of communities on the route is an exact match for the set of communities in one of the statements in the community list.

no match community

To delete a match term from a route map, use the **no match community** command. The command **no match community list exact-match** removes the match statement from the route map. (It does not simply remove the exact-match option.) The command **no match community** removes the match term and all its community lists.

Format	`no match community` *`community-list`* `[`*`community-list...`*`] [exact-match]`
Mode	Route Map Configuration

match ip address

To configure a route map to match based on a destination prefix, use the **match ip address** command in Route Map Configuration mode. If you specify multiple prefix lists in one statement, then a match occurs if a prefix matches any one of the prefix lists. If you configure a match IP address statement within a route map section that already has a match IP address statement, the new prefix lists are added to the existing set of prefix lists, and a match occurs if any prefix list in the combined set matches the prefix.

Default	No match criteria are defined by default.
Format	`match ip address prefix-list` *`prefix-list-name`* `[`*`prefix-list-name...`*`]`
Mode	Route Map Configuration

Parameter	Description
prefix-list-name	The name of a prefix list used to identify the set of matching routes. Up to eight prefix lists can be specified.

no match ip address (for a prefix list)

To delete a match statement for a prefix list from a route map, use the **no match ip address** command.

Format	`no match ip address prefix-list` *`prefix-list-name`* `[`*`prefix-list-name...`*`]`
Mode	Route Map Configuration

match ip address {access-list-number | access-list-name}

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 {`*`access-list-number`* `|` *`access-list-name`*`}` `[...`*`access-list-number`* `|` *`access-list-name`*`]`
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 Routing) (config)#access-list 1 permit ip 10.1.0.0 0.0.255.255
(NETGEAR Routing) (config)#access-list 2 permit ip 10.2.0.0 0.0.255.255
(NETGEAR Routing) (config)#route-map equal-access permit 10
(NETGEAR Routing) (config-route-map)#match ip address 1
(NETGEAR Routing) (config-route-map)#set ip default next-hop 192.168.6.6
(NETGEAR Routing) (config-route-map)#route-map equal-access permit 20
(NETGEAR Routing) (config-route-map)#match ip address 2
(NETGEAR Routing) (config-route-map)#set ip default next-hop 172.16.7.7
(NETGEAR Routing) (config)#interface 1/0/1
(NETGEAR Routing) (Interface 1/0/1)#ip address 10.1.1.1 255.255.255.0
(NETGEAR Routing) (Interface 1/0/1)#ip policy route-map equal-access
(NETGEAR Routing) (config)#interface 1/0/2
(NETGEAR Routing) (Interface 1/0/2)#ip address 192.168.6.5 255.255.255.0
(NETGEAR Routing) (config)#interface 1/0/3
(NETGEAR Routing) (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 router 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 router 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 Routing) #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

NETGEAR Routing) #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 Routing) #
(NETGEAR Routing) #
(NETGEAR Routing) #configure
(NETGEAR Routing) (Config)#route-map madan
(NETGEAR Routing) (route-map)#match ip address 1 2 3 4 5 madan
(NETGEAR Routing) (route-map)#match mac-list madan mohan goud
(NETGEAR Routing) (route-map)#exit
(NETGEAR Routing) (Config)#exit
(NETGEAR Routing) #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 Routing) (Config)#access-list 2 permit every
Request denied. Another application using this ACL restricts the number of rules allowed.
(NETGEAR Routing) (Config)#ip access-list madan
(NETGEAR Routing) (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 [`*`access-list-number`* `|` *`access-list-name`*`]`
Mode	Route Map Configuration

match ipv6 address

Use this command to configure a route map to match based on a destination prefix. The *prefix-list-name* identifies the name of an IPv6 prefix list used to identify the set of matching routes. Up to eight prefix lists may be specified. If multiple prefix lists are specified, a match occurs if a prefix matches any one of the prefix lists. If you configure a match ipv6 address statement within a route map section that already has a match ipv6 address statement, the new prefix lists are added to the existing set of prefix lists, and a match occurs if any prefix list in the combined set matches the prefix.

Default	No match criteria are defined by default.
Format	`match ipv6 address prefix-list` *`prefix-list-name`* `[`*`prefix-list-name...`*`]`
Mode	Route Map Configuration

Command example:

The following example matches IPv6 addresses that are specified by the prefix list apple through the route map abc:

```
Router(config)# route-map abc
Router(config-route-map)# match ipv6 address prefix-list apple
```

no match ipv6 address

To delete a match statement from a route map, use the **no match ipv6 address** command.

Format	no match ipv6 address prefix-list *prefix-list-name* [*prefix-list-name...*]]
Mode	Route Map Configuration

match length

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	match length *min max*
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	no match length
Mode	Route Map Configuration

match mac-list

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 MAC ACL configuration are applied with other actions involved in 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.

Default	No match criteria are defined by default.
Format	match mac-list *mac-list-name* [*mac-list-name*]
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 Routing) (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 Routing) #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 Routing) #
(NETGEAR Routing) #
(NETGEAR Routing) #configure
(NETGEAR Routing) (Config)#route-map madan
(NETGEAR Routing) (route-map)#match mac-list madan mohan goud
(NETGEAR Routing) (route-map)#exit
(NETGEAR Routing) (Config)#exit
(NETGEAR Routing) #show route-map

route-map madan permit 10
     Match clauses:
       mac-list (access-lists) : madan mohan goud
     Set clauses:

(NETGEAR Routing) (Config)#mac access-list extended madan
(NETGEAR Routing) (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

set as-path

To prepend one or more AS numbers to the AS path in a BGP route, use the **set as-path** command in Route Map Configuration mode. This command is normally used to insert one or more instances of the local AS number at the beginning of the AS_PATH attribute of a BGP route. Doing so increases the AS path length of the route. The AS path length has a strong influence on BGP route selection. Changing the AS path length can influence route selection on the local router or on routers to which the route is advertised.

When prepending an inbound route, if the first segment in the AS_PATH of the received route is an AS_SEQUENCE, *as-path-string* is inserted at the beginning of the sequence. If the first segment is an AS_SET, *as-path-string* is added as a new segment with type AS_SEQUENCE at the beginning of the AS path. When prepending an outbound route to an external peer, *as-path-string* follows the local AS number, which is always the first ASN.

Format	set as-path prepend *as-path-string*
Mode	Route Map Configuration

Parameter	Description
as-path-string	A list of AS path numbers to insert at the beginning of the AS_PATH attribute of matching BGP routes. To prepend more than one AS number, separate the ASNs with a space and enclose the string in quotes. Up to ten AS numbers may be prepended.

Command example:

The following example prepends three instances of an external peer's AS number to paths that are received from that peer, causing routes that are learned from this peer less likely to be chosen as the best path:

```
(NETGEAR Switch)# config
(NETGEAR Switch)# route-map ppAsPath
(NETGEAR Switch)# set as-path prepend “2 2 2”
(NETGEAR Switch)# exit
(NETGEAR Switch)# router bgp 1
(NETGEAR Switch)# neighbor 172.20.1.2 remote-as 2
(NETGEAR Switch)# neighbor 172.20.1.2 route-map ppAsPath in
```

no set as-path

To remove a set command from a route map, use the **no set as-path** command.

Format	no set as-path prepend *as-path-string*
Mode	Route Map Configuration

set comm-list delete

To remove BGP communities from an inbound or outbound UPDATE message, use the **set comm-list delete** command in Route Map Configuration mode. A route map with this **set** command can be used to remove selected communities from inbound and outbound routes. When a community list is applied to a route for this purpose, each of the route's communities is submitted to the community list one at a time. Communities permitted by the list are removed from the route. Because communities are processed individually, a community list used to remove communities should not include the exact-match option on statements with multiple communities. Such statements can never match an individual community.

When a route map statement includes both `set community` and `set comm-list delete` terms, the `set comm-list delete` term is processed first, and then the `set community` term (meaning that, communities are first removed, and then communities are added).

Format	set comm-list *community-list-name* delete
Mode	Route Map Configuration

Parameter	Description
community-list-name	A standard community list name.

no set comm-list

To delete the set command from a route map, use the **no set comm-list** command.

Format	no set comm-list
Mode	Route Map Configuration

set community

To modify the communities attribute of matching routes, use the **set community** command in Route Map Configuration mode. The **set community** command can be used to assign communities to routes originated through BGP's network and redistribute commands, and to set communities on routes received from a specific neighbor or advertised to a specific neighbor. It can also be used to remove all communities from a route.

To remove a subset of the communities on a route, use the command *set comm-list delete* on page 705.

Format	`set community {`*`community-number`* `[additive] | none}`
Mode	Route Map Configuration

Parameter	Description
community-number	One to sixteen community numbers, either as a 32-bit integers or in AA:NN format. Communities are separated by spaces. The well-known communities no advertise and no-export are also accepted.
additive	(Optional) Communities are added to those already attached to the route.
none	(Optional) Removes all communities from matching routes.

no set community

To remove a set term from a route map, use the **`no set community`** command.

Format	`no set community`
Mode	Route Map Configuration

set interface

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 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	`set interface null0`
Mode	Route Map Configuration

set ip next-hop

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 router.

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.

Format	`set ip next-hop` *`ip-address`* `[...`*`ip-address`*`]`
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. A maximum of 16 next-hop IP addresses can be specified in this se clause.

no set ip next-hop

Use this command to remove a set command from a route map.

Format	`no set ip next-hop` *`ip-address`* `[...`*`ip-address`*`]`
Mode	Route Map Configuration

set ip default next-hop

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 router 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 explicit route for the packet's destination address 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 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.

Format	`set ip default next-hop` *`ip-address`* `[...`*`ip-address`*`]`
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. A maximum of 16 next-hop IP addresses can be specified in this set clause.

no set ip default next-hop

Use this command to remove a set command from a route map.

Format	`no set ip default next-hop` *`ip-address`* [*`...ip-address`*]
Mode	Route Map Configuration

set ip precedence

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).

Format	`set ip precedence` *`value`*
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	`no set ip precedence`
Mode	Route Map Configuration

set ipv6 next-hop (BGP)

To set the IPv6 next hop of a route, use the **`set ipv6 next-hop`** command in Route Map Configuration mode. When used in a route map applied to UPDATE messages received from a neighbor, the command sets the next hop address for matching IPv6 routes received from the neighbor.

When used in a route map applied to UPDATE messages sent to a neighbor, the command sets the next hop address for matching IPv6 routes sent to the neighbor. If the address is a link local address, the address is assumed to be on the interface where the UPDATE is sent or received. If the command specifies a global IPv6 address, the address is not required to be on a local subnet.

Format	`set ipv6 next-hop` *`ipv6-address`*
Mode	Route Map Configuration

Parameter	Description
ipv6-address	The IPv6 address set as the Network Address of Next Hop field in the MP_NLRI attribute of an UPDATE message.

no set ipv6 next-hop (BGP)

To remove a **set** command from a route map, use the **`no set ipv6 next-hop`** command.

Format	`no set ipv6 next-hop`
Mode	Route Map Configuration

set local-preference

To set the local preference of specific BGP routes, use the **`set local-preference`** command in Route Map Configuration mode. The local preference is the first attribute used to compare BGP routes. Setting the local preference can influence which route BGP selects as the best route. When used in conjunction with a *match as-path* or *match ip address* command, this command can be used to prefer routes that transit certain ASs or to make the local router a more preferred exit point to certain destinations.

Format	`set local-preference` *`value`*
Mode	Route Map Configuration

Parameter	Description
value	A local preference value, from 0 to 4,294,967,295 (any 32-bit integer).

no set local-preference

To remove a set command from a route map, use the **no** form of this command.

Format	`no set local-preference` *`value`*
Mode	Route Map Configuration

set metric (BGP)

To set the metric of a route, use the **set metric** command in Route Map Configuration mode. This command sets the Multi Exit Discriminator (MED) when used in a BGP context. When there are multiple peering points between two autonomous systems (AS), setting the MED on routes advertised by one router can influence the other AS to send traffic through a specific peer.

Format	set metric *value*
Mode	Route Map Configuration

Parameter	Description
value	A metric value, from 0 to 4,294,967,295 (any 32-bit integer).

no set metric (BGP)

To remove a **set** command from a route map, use the **no set metric** command.

Format	no set metric *value*
Mode	Route Map Configuration

show ip policy

This command lists the route map associated with each interface.

Format	show ip policy
Mode	Privileged Exec

Term	Definition
Interface	The interface.
Route-map	The route map

show ip prefix-list

This command displays configuration and status for a prefix list.

Format	show ip prefix-list [detail | summary] *prefix-list-name* [*network/length*] [seq *sequence-number*] [longer] [first-match]
Mode	Privileged EXEC

Parameter	Description
detail | summary	(Optional) Displays detailed or summarized information about all prefix lists.
prefix-list-name	(Optional) The name of a specific prefix list.
network/length	(Optional) The network number and length (in bits) of the network mask.
seq	(Optional) Applies the sequence number to the prefix list entry.
sequence-number	(Optional) The sequence number of the prefix list entry.
longer	(Optional) Displays all entries of a prefix list that are more specific than the given network/length.
first-match	(Optional) Displays the entry of a prefix list that matches the given network/length.

Acceptable forms of this command are as follows:

- **show ip prefix-list** *prefix-list-name network/length* **first-match**
- **show ip prefix-list** *prefix-list-name network/length* **longer**
- **show ip prefix-list** *prefix-list-name network/length*
- **show ip prefix-list** *prefix-list-name* **seq** *sequence-number*
- **show ip prefix-list** *prefix-list-name*
- **show ip prefix-list summary**
- **show ip prefix-list summary** *prefix-list-name*
- **show ip prefix-list detail**
- **show ip prefix-list detail** *prefix-list-name*

Command example:

```
(NETGEAR Switch) #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 ipv6 prefix-list

This command displays configuration and status for a selected prefix list.

Format	`show ipv6 prefix-list [detail | summary] listname [ipv6-prefix/prefix-length] [seq sequence-number] [longer] [first-match]`
Mode	Privileged EXEC

Parameter	Description
detail | summary	(Optional) Displays detailed or summarized information about all prefix lists.
list-name	(Optional) The name of a specific prefix list.
ipv6-prefix/prefix-length	(Optional) The network number and length (in bits) of the network mask.
seq	(Optional) Applies the sequence number to the prefix list entry.
sequence-number	(Optional) The sequence number of the prefix list entry.
longer	(Optional) Displays all entries of a prefix list that are more specific than the given network/length.
first-match	(Optional) Displays the entry of a prefix list that matches the given network/length.

Acceptable forms of this command are as follows:

- **show ipv6 prefix-list** *listname ipv6-prefix/prefix-length* **first-match**
- **show ipv6 prefix-list** *listname ipv6-prefix/prefix-length* **longer**
- **show ipv6 prefix-list** *listname ipv6-prefix/prefix-length*
- **show ipv6 prefix-list** *listname* **seq** *sequence-number*
- **show ipv6 prefix-list** *listname*
- **show ipv6 prefix-list summary**
- **show ipv6 prefix-list summary** *listname*
- **show ipv6 prefix-list detail**
- **show ipv6 prefix-list detail** *listname*

The command outputs the following information.

Parameter	Description
count	Number of entries in the prefix list.
range entries	Number of entries that match the input range.
ref count	Number of entries referencing the given prefix list.
seq	Sequence number of the entry in the list.
permit/deny	The action to take.
sequences	Range of sequence numbers for the entries in the list
hit count	Number of matches for the prefix entry

Command example:

```
(NETGEAR Switch) #show ipv6 prefix-list apple
ipv6 prefix-list apple:
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 apple
ipv6 prefix-list apple:
count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
```

Command example:

```
(NETGEAR Switch) #show ipv6 prefix-list detail apple
ipv6 prefix-list apple:
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)
```

show route-map

To display a route map, use the **show route-map** command in Privileged EXEC mode.

Format	show route-map [*map-name*]
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
```

clear ip prefix-list

To reset IP prefix-list counters, use the **clear ip prefix-list** command in Privileged EXEC mode. This command is used to clear prefix-list hit counters. The hit count is a value indicating the number of matches to a specific prefix list entry.

Format	clear ip prefix-list [*prefix-list-name*] [*network/length*]
Mode	Privileged EXEC

Parameter	Description
prefix-list-name	(Optional) Name of the prefix list from which the hit count is to be cleared.
network/length	(Optional) Network number and length (in bits) of the network mask. If this option is specified, hit counters are only cleared for the matching statement.

Command example:

```
(NETGEAR Switch) # clear ip prefix-list orange 20.0.0.0/8
```

clear ipv6 prefix-list

Use this command to reset and clear IPv6 prefix-list hit counters. The hit count is a value indicating the number of matches to a specific prefix list entry.

Format	clear ipv6 prefix-list [*prefix-list-name*] [*ipv6-prefix/prefix-length*]
Mode	Privileged EXEC

Parameter	Description
list-name	(Optional) Name of the prefix list from which the hit count is to be cleared.
ipv6-prefix/prefix-length	(Optional) IPv6 prefix number and length (in bits) of the network mask. If this option is specified, hit counters are only cleared for the matching statement.

Router Discovery Protocol Commands

This section describes the commands you use to view and configure Router Discovery Protocol settings on the switch. The Router Discovery Protocol enables a host to discover the IP address of routers on the subnet.

ip irdp

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

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` *`ipaddr`*
Mode	Interface Config

no ip irdp address

This command configures the default address used to advertise the router for the interface.

Format	`no ip irdp address`
Mode	Interface Config

ip irdp holdtime

This command configures the value of the holdtime field of the router advertisement sent from this interface. The *seconds* argument holdtime value is in the range of 4 to 9000 seconds.

Default	3 * maxinterval
Format	`ip irdp holdtime` *seconds*
Mode	Interface Config

no ip irdp holdtime

This command resets the default value of the holdtime field of the router advertisement sent from this interface.

Format	`no ip irdp holdtime`
Mode	Interface Config

ip irdp maxadvertinterval

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` *seconds*
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

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 seconds`
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

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 ip address`
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

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 number`
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

This command displays the router discovery information for all interfaces, a specified interface, or specified VLAN. The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vland-id* argument are used to specify the VLAN ID of the routing VLAN directly instead of in a *unit/slot/port* format. The *vland-id* argument can be a number from 1–4093.

Format	`show ip irdp {`*unit/slot/port* `| vlan` *vland-id* `| all}`
Modes	Privileged EXEC User EXEC

Term	Definition
Interface	The *unit/slot/port* that corresponds to a physical routing interface or VLAN routing interface.
vlan	Use this keyword to specify the VLAN ID of the routing VLAN directly instead of in a *unit/slot/port* format.
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

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 *unit/slot/port* 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 *unit/slot/port* for the VLAN interface stays the same across a restart. Keeping the *unit/slot/port* the same ensures that the correct interface configuration is applied to each interface when the system restarts.

Format	`vlan routing` *vlanid* [*interface-id*]
Mode	VLAN Config

no vlan routing

This command deletes routing on a VLAN.

Format	`no vlan routing` *vlanid*
Mode	VLAN Config

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 *unit/slot/port* for the VLAN routing interface. In this example, *unit/slot/port* is 4/51 for 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

           Logical
VLAN ID   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

           Logical
VLAN ID   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 XCM8900"
!System Up Time          "0 days 8 hrs 38 mins 3 secs"
```

```
!Cut-through mode is configured as disabled
!Additional Packages     NETGEAR BGP-4,NETGEAR QOS,NETGEAR Multicast,NETGEAR
IPv6,NETGEAR IPv6 Management,NETGEAR Metro,NETGEAR Routing,NETGEAR Data Center
!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
router ospf
exit
ipv6 router ospf
exit
exit
```

interface vlan

Use this command to enter Interface configuration mode for the specified VLAN. The vlan-id range is 1 to 4093.

Format	`interface vlan` *`vlan-id`*
Mode	Global Config

show ip vlan

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 *unit/slot/port* 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

This section describes the commands you use to view and configure Virtual Router Redundancy Protocol (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)

Use this command in Global Config mode to enable the administrative mode of VRRP on the router.

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 router.

Format	`no ip vrrp`
Mode	Global Config

ip vrrp (Interface Config)

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` ***vrid***
Mode	Interface Config

ip vrrp mode

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` *vrid* `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` *vrid* `mode`
Mode	Interface Config

ip vrrp ip

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` *vrid* `ip` *ipaddr* `[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

Use this command to allow the VRRP Master 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 Master 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

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

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

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 master. 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 master. If the master 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 master's priority, the router will take over as master 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	`ip vrrp` *`vrid`* `priority` *`priority`*
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	`no ip vrrp` *vrid* `priority`
Mode	Interface Config

ip vrrp timers advertise

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	`ip vrrp` *vrid* `timers advertise` *seconds*
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	`no ip vrrp` *vrid* `timers advertise`
Mode	Interface Config

ip vrrp track interface

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 directly instead of in a *unit/slot/port* format. The *vlan-id* can be a number from 1–4093.

When the tracked interface is down or the interface has been removed from the router, the priority of the VRRP router will be decremented by the value specified in the *priority* argument. When the interface is up for IP protocol, the priority will be incremented by the *priority* value.

A VRRP configured interface can track more than one interface. When a tracked interface goes down, then the priority of the router will be decreased by 10 (the default priority

decrement) for each downed interface. 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 giving the optional priority, then the default priority will be set. The default priority decrement is 10.

Default	priority: 10
Format	ip vrrp *vrid* track interface {*unit/slot/port* | *vlan vlan-id*} [decrement *priority]*
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	no ip vrrp *vrid* track interface {*unit/slot/port* | *vlan vlan-id*} [decrement]
Mode	Interface Config

ip vrrp track ip route

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, then the priority of the router will be decreased by 10 (the default priority decrement) for each downed route. By default no routes are tracked. If you specify just the route to be tracked, without giving the optional priority, then the default priority will be set. The default priority decrement is 10. The default priority decrement is changed using the *priority* argument.

Default	priority: 10
Format	ip vrrp *vrid* track ip route *ip-address/prefix-length* [decrement *priority*]
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	`no ip vrrp vrid track interface unit/slot/port [decrement]`
Mode	Interface Config

show ip vrrp interface stats

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 directly instead of in a *unit/slot/port* format. 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 virtual router state has changed to MASTER.
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.

Term	Definition
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 ip vrrp

This command displays whether VRRP functionality is enabled or disabled on the switch. It also displays some global parameters which are required for monitoring. This command takes no options.

Format	`show ip vrrp`
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

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 directly instead of in a *unit/slot/port* format. The *vlan-id* can be a number from 1–4093.

Format	`show ip vrrp interface {`*unit/slot/port* `|` `vlan` *vlan-id*`}` *vrid*
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 **ip vrrp** *vrid* **priority** *priority* 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 Master can accept ping packets sent to one of the virtual router's IP addresses.
State	The state (Master/backup) 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

This command displays information about each virtual router configured on the switch. This command takes no options. It displays information about each virtual router.

Format	`show ip vrrp interface brief`
Modes	Privileged EXEC User EXEC

Term	Definition
Interface	*unit/slot/port*
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 (Master/backup) of the virtual router.

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

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

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

This command configures the minimum wait time in seconds for BootP/DHCP Relay on the system. 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` *seconds*
Mode	Global Config

no bootpdhcprelay minwaittime

This command configures the default minimum wait time in seconds for BootP/DHCP Relay on the system.

Format	`no bootpdhcprelay minwaittime`
Mode	Global Config

show bootpdhcprelay

This command displays the BootP/DHCP Relay information.

Format	`show bootpdhcprelay`
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 relaying of requests is enabled or disabled.
Circuit Id Option Mode	The DHCP circuit Id option which may be enabled or disabled.

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 10. 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
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 a given 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.

clear ip helper statistics

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
```

ip helper-address (Global Config)

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 given UDP port number or to specify multiple UDP port numbers handled by a specific server.

Default	`No helper addresses are configured.`
Format	`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]`
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	The destination UDP port may be optionally specified by its name. Whether a port is specified by its number or its name has no effect on behavior. 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 [*server-address*] [*dest-udp-port* | 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)

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 given port number or to specify multiple port numbers handled by a specific server.

Default	No helper addresses are configured.
Format	ip helper-address {*server-address* | discard} [*dest-udp-port* | 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.
port-name	The destination UDP port may be optionally specified by its name. Whether a port is specified by its number or its name has no effect on behavior. 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
(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 [`*`server-address`*` | discard] [`*`dest-udp-port`*` | dhcp | domain | isakmp | mobile ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]`
Mode	Interface Config

ip helper enable

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 **bootpdhcprelay 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

Use this command to display the IP helper address configuration. The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing 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 directly instead of in a *unit/slot/port* format. The *vlan-id* can be a number from 1–4093.

Format	`show ip helper-address [`*unit/slot/port* `|` `vlan` *vlan-id*`]`
Mode	Privileged EXEC

Parameter	Description
interface	The relay configuration is applied to packets that arrive on this interface. This field is set to any 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 any are applied to packets with the destination UDP ports listed in Table 4.
Discard	If Yes, packets arriving on the given interface with the given 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

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 bootpdhcprelay. 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 bootpdhcprelay. 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
```

Open Shortest Path First Commands

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 741
- *OSPF Interface Commands* on page 762
- *IP Event Dampening Commands* on page 768
- *OSPFv2 Stub Router Commands* on page 773
- *OSPF Show Commands* on page 775

The following switches support OSPF:

- M6100
- M5300-28G3
- M5300-52G3
- M5300-28GF3

The following switches support OSPF with an L3 license:

- M5300-28G
- M5300-52G
- M5300-28G-POE+
- M5300-52G-POE+

General OSPF Commands

router ospf

Use this command to enter Router OSPF mode.

Format	`router ospf`
Mode	Global Config

enable (OSPF)

This command resets the default administrative mode of OSPF in the router (active).

Default	enabled
Format	`enable`
Mode	Router OSPF Config

no enable (OSPF)

This command sets the administrative mode of OSPF in the router to inactive.

Format	`no enable`
Mode	Router OSPF Config

network area (OSPF)

Use this command to enable OSPFv2 on an interface and set its area ID if the IP address of an interface is covered by this network command.

Default	disabled
Format	`network` *`ip-address wildcard-mask`* `area` *`area-id`*
Mode	Router OSPF Config

no network area (OSPF)

Use this command to disable the OSPFv2 on a interface if the IP address of an interface was earlier covered by this network command.

Format	`no network` *`ip-address wildcard-mask`* `area` *`area-id`*
Mode	Router OSPF Config

1583compatibility

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, OSPF 1583 compatibility mode should be disabled.

Default	enabled

Format	`1583compatibility`
Mode	Router OSPF Config

no 1583compatibility

This command disables OSPF 1583 compatibility.

Format	`no 1583compatibility`
Mode	Router OSPF Config

area default-cost (OSPF)

This command configures the default cost for the stub area. For the *value* argument, you must specify an integer value between 1–16777215.

Format	`area` *`area-id`* `default-cost` *`value`*
Mode	Router OSPF Config

area nssa (OSPF)

This command configures the specified *area-id* to function as an NSSA.

Format	`area` *`area-id`* `nssa`
Mode	Router OSPF Config

no area nssa

This command disables nssa from the specified area id.

Format	`no area` *`area-id`* `nssa`
Mode	Router OSPF Config

area nssa default-info-originate (OSPF)

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	`area` *`area-id`* `nssa default-info-originate [`*`metric`*`] [comparable | non-comparable]`
Mode	Router OSPF Config

no area nssa default-info-originate (OSPF)

This command disables the default route advertised into the NSSA.

Format	`no area` *`area-id`* `nssa default-info-originate [`*`metric`*`] [comparable | non-comparable]`
Mode	Router OSPF Config

area nssa no-redistribute (OSPF)

This command configures the NSSA Area Border router (ABR) so that learned external routes will not be redistributed to the NSSA.

Format	`area` *`area-id`* `nssa no-redistribute`
Mode	Router OSPF Config

no area nssa no-redistribute (OSPF)

This command disables the NSSA ABR so that learned external routes are redistributed to the NSSA.

Format	`no area` *`area-id`* `nssa no-redistribute`
Mode	Router OSPF Config

area nssa no-summary (OSPF)

This command configures the NSSA so that summary LSAs are not advertised into the NSSA.

Format	`area` *`area-id`* `nssa no-summary`
Mode	Router OSPF Config

no area nssa no-summary (OSPF)

This command disables nssa from the summary LSAs.

Format	`no area` *`area-id`* `nssa no-summary`
Mode	Router OSPF Config

area nssa translator-role (OSPF)

This command configures the translator role of the NSSA. The **`always`** keyword causes the router to assume the role of the translator the instant it becomes a border router; The and the **`candidate`** keyword causes the router to participate in the translator election process when it attains border router status.

Format	`area area-id nssa translator-role {always | candidate}`
Mode	Router OSPF Config

no area nssa translator-role (OSPF)

This command disables the nssa translator role from the specified area id.

Format	`no area area-id nssa translator-role {always | candidate}`
Mode	Router OSPF Config

area nssa translator-stab-intv (OSPF)

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 area-id nssa translator-stab-intv stabilityinterval`
Mode	Router OSPF Config

no area nssa translator-stab-intv (OSPF)

This command disables the nssa translator's *stabilityinterval* from the specified area id.

Format	`no area area-id nssa translator-stab-intv stabilityinterval`
Mode	Router OSPF Config

area range (OSPF)

Use the area range 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	`area area-id range ip-address netmask {summarylink | nssaexternallink} [advertise | not-advertise] [cost cost]`
Mode	OSPFv2 Router Configuration

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.

Parameter	Description
summarylink	When this keyword is given, the area range is used when summarizing prefixes advertised in type 3 summary LSAs.
nssaexternallink	When this keyword is given, the area range is used when translating type 7 LSAs to type 5 LSAs.
advertise	[Optional] When this keyword is given, the summary prefix is advertised when the area range is active. This is the default.
not-advertise	[Optional] When this keyword is given, neither the summary prefix nor the contained prefixes are advertised when the area range is active. When the not-advertise option is given, any static cost previously configured is removed from the system configuration.
cost	[Optional] If an optional cost is given, 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

The **no area range** command deletes a specified area range or reverts an option to its default.

Format	`no area` *`area-id`* `range` *`prefix netmask`* `{summarylink | nssaexternallink} [advertise | not-advertise] [cost]`
Mode	OSPFv2 Router Configuration

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 (OSPF)

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	`area` *`area-id`* `stub`
Mode	Router OSPF Config

no area stub

This command deletes a stub area for the specified area ID.

Format	`no area` *`area-id`* `stub`
Mode	Router OSPF Config

area stub no-summary (OSPF)

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` *`area-id`* `stub no-summary`
Mode	Router OSPF Config

no area stub no-summary

This command configures the default Summary LSA mode for the stub area identified by *`area-id`*.

Format	`no area` *`area-id`* `stub no-summary`
Mode	Router OSPF Config

area virtual-link (OSPF)

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 *area-id* virtual-link *neighbor*
Mode	Router OSPF Config

no area virtual-link

This command deletes the OSPF virtual interface from the given interface, identified by *area-id* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Format	no area *area-id* virtual-link *neighbor*
Mode	Router OSPF Config

area virtual-link authentication

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 *area-id* virtual-link *neighbor* authentication {none | simple *key*| encrypt *key keyid*}
Mode	Router OSPF Config

no area virtual-link authentication

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 *area-id* virtual-link *neighbor* authentication
Mode	Router OSPF Config

area virtual-link dead-interval (OSPF)

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` *area-id* `virtual-link` *neighbor* `dead-interval` *seconds*
Mode	Router OSPF Config

no area virtual-link dead-interval

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` *area-id* `virtual-link` *neighbor* `dead-interval`
Mode	Router OSPF Config

area virtual-link hello-interval (OSPF)

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	`area` *area-id* `virtual-link` *neighbor* `hello-interval` *1-65535*
Mode	Router OSPF Config

no area virtual-link hello-interval

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	`no area` *area-id* `virtual-link` *neighbor* `hello-interval`
Mode	Router OSPF Config

area virtual-link retransmit-interval (OSPF)

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	area *area-id* virtual-link *neighbor* retransmit-interval *seconds*
Mode	Router OSPF Config

no area virtual-link retransmit-interval

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	no area *area-id* virtual-link *neighbor* retransmit-interval
Mode	Router OSPF Config

area virtual-link transmit-delay (OSPF)

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	area *area-id* virtual-link *neighbor* transmit-delay *seconds*
Mode	Router OSPF Config

no area virtual-link transmit-delay

This command resets the default transmit delay for the OSPF virtual interface to the default value.

Format	no area *area-id* virtual-link *neighbor* transmit-delay
Mode	Router OSPF Config

auto-cost (OSPF)

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 (ref_bw / 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	`auto-cost reference-bandwidth` *mbps*
Mode	Router OSPF Config

no auto-cost reference-bandwidth (OSPF)

Use this command to set the reference bandwidth to the default value.

Format	`no auto-cost reference-bandwidth`
Mode	Router OSPF Config

capability opaque

Use this command to enable Opaque Capability on the Router. The information contained in Opaque LSAs may be used directly by OSPF or indirectly by an application wishing to distribute information throughout the OSPF domain. NETGEAR Managed Switch supports the storing and flooding of Opaque LSAs of different scopes. The default value of `enabled` means that OSPF will forward opaque LSAs by default. If you want to upgrade from a previous release, where the default was disabled, opaque LSA forwarding will be enabled. If you want to disable opaque LSA forwarding, then you should enter the command no capability opaque in OSPF router configuration mode after the software upgrade.

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

Use this command to disable and re-enable OSPF.

Format	`clear ip ospf`
Mode	Privileged EXEC

clear ip ospf configuration

Use this command to reset the OSPF configuration to factory defaults.

Format	`clear ip ospf configuration`
Mode	Privileged EXEC

clear ip ospf counters

Use this command to reset global and interface statistics.

Format	`clear ip ospf counters`
Mode	Privileged EXEC

clear ip ospf neighbor

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	`clear ip ospf neighbor [`*neighbor-id*`]`
Mode	Privileged EXEC

clear ip ospf neighbor interface

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 on a specific interface, use the optional parameter *neighbor-id*.

Format	`clear ip ospf neighbor interface [`*unit/slot/port*`] [`*neighbor-id*`]`
Mode	Privileged EXEC

clear ip ospf redistribution

Use this command to flush all self-originated external LSAs. Reapply the redistribution configuration and reoriginate prefixes as necessary.

Format	`clear ip ospf redistribution`
Mode	Privileged EXEC

default-information originate (OSPF)

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 metric] [metric-type {1 | 2}]`
Mode	Router OSPF Config

no default-information originate (OSPF)

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 (OSPF)

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 metric`
Mode	Router OSPF Config

no default-metric (OSPF)

This command is used to reset the default for the metric of distributed routes.

Format	`no default-metric`
Mode	Router OSPF Config

distance ospf (OSPF)

This command sets the route preference value of OSPF in the router. 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	`distance ospf {intra-area preference | inter-area preference | external preference}`
Mode	Router OSPF Config

no distance ospf

This command resets the default route preference value of OSPF routes in the router. The type of OSPF route can be **intra-area**, **inter-area**, or **external**.

Format	no distance ospf {intra-area | inter-area | external}
Mode	Router OSPF Config

distribute-list out (OSPF)

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	distribute-list *access-list* out {rip | bgp | static | connected}
Mode	Router OSPF Config

no distribute-list out

Use this command to reset the access list to filter routes received from the source protocol.

Format	no distribute-list *access-list* out {rip | bgp | static | connected}
Mode	Router OSPF Config

exit-overflow-interval (OSPF)

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 will not leave overflow state until restarted. The range for the *seconds* argument is 0 to 2147483647 seconds.

Default	0
Format	exit-overflow-interval *seconds*
Mode	Router OSPF Config

no exit-overflow-interval

This command configures the default exit overflow interval for OSPF.

Format	no exit-overflow-interval
Mode	Router OSPF Config

external-lsdb-limit (OSPF)

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 it database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area. The range for the *limit* argument is -1 to 2147483647.

Default	-1
Format	`external-lsdb-limit` *limit*
Mode	Router OSPF Config

no external-lsdb-limit

This command configures the default external LSDB limit for OSPF.

Format	`no external-lsdb-limit`
Mode	Router OSPF Config

log-adjacency-changes

To enable logging of OSPFv2 neighbor state changes, use the log-adjacency-changes command in router configuration mode. State changes are logged with INFORMATIONAL severity.

Default	Adjacency state changes are logged, but without the detail option.
Format	`log-adjacency-changes [detail]`
Mode	OSPFv2 Router Configuration

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

Use the no form of the command to disable state change logging.

Format	`no log-adjacency-changes [detail]`
Mode	OSPFv2 Router Configuration

prefix-suppression (Router OSPF Config)

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

This command disables prefix-suppression. No prefixes are suppressed from getting advertised.

Format	`no prefix-suppression`
Mode	Router OSPF Config

prefix-suppression (Router OSPFv3 Config)

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	`prefix-suppression`
Mode	Router OSPFv3 Config

no prefix-suppression

This command disables prefix-suppression. No prefixes are suppressed from getting advertised.

Format	`no prefix-suppression`
Mode	Router OSPFv3 Config

router-id (OSPF)

This command sets a 4-digit dotted-decimal number uniquely identifying the router ospf id. The *ipaddress* is a configured value.

Format	`router-id` *ipaddress*
Mode	Router OSPF Config

redistribute (OSPF)

This command configures the OSPF protocol to allow redistribution of routes from the specified source protocol or routers. The *metric* argument can be in the range 0–16777214. The **metric type** can be 1 or 2. The *tag* argument can be in the range 0–4294967295.

Default	metric—unspecified type—2 tag—0
Format	`redistribute {rip | bgp | static | connected} [metric` *metric*`] [metric-type {1 | 2}] [tag` *tag*`] [subnets]`
Mode	Router OSPF Config

no redistribute

This command configures OSPF protocol to prohibit redistribution of routes from the specified source protocol or routers.

Format	`no redistribute {rip | bgp | static | connected} [metric] [metric-type] [tag] [subnets]`
Mode	Router OSPF Config

maximum-paths (OSPF)

This command sets the number of paths that OSPF can report for a given destination in which *maxpaths* is platform dependent.

Default	4
Format	`maximum-paths` *maxpaths*
Mode	Router OSPF Config

no maximum-paths

This command resets the number of paths that OSPF can report for a given destination back to its default value.

Format	`no maximum-paths`
Mode	Router OSPF Config

passive-interface default

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	`passive-interface default`
Mode	Router OSPF Config

no passive-interface default

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 (OSPF)

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 directly instead of in a *`unit/slot/port`* format. The *`vlan-id`* can be a number from 1–4093.

Default	disabled
Format	`passive-interface {`*`unit/slot/port`*` | vlan `*`vlan-id`*`}`
Mode	Router OSPF Config

no passive-interface

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 directly instead of in a *`unit/slot/port`* format. The *`vlan-id`* can be a number from 1–4093.

Format	`no passive-interface {`*`unit/slot/port`* `| vlan` *`vlan-id`*`}`
Mode	Router OSPF Config

timers pacing flood

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 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	`timers pacing flood` *`milliseconds`*
Mode	OSPFv2 Router Configuration

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

To revert LSA transmit pacing to the default rate, use the no timers pacing flood command.

Format	`no timers pacing flood`
Mode	OSPFv2 Router Configuration

timers pacing lsa-group (OSPF)

To adjust how OSPF groups LSAs for periodic refresh, use the timers pacing lsa-group command in OSPFv2 Router Configuration 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	`timers pacing lsa-group` *`seconds`*
Mode	OSPFv2 Router Configuration

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.

timers spf

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 0–65535 seconds.

Default	delay-time—5 hold-time—10
Format	`timers spf` *`delay-time hold-time`*
Mode	Router OSPF Config

trapflags (OSPF)

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 11. 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
overflow	• lsdb-overflow • lsdb-approaching-overflow

Table 11. Trapflags groups

Group	Flags
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	`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}}`
Mode	Router OSPF Config

no trapflags

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	`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}}`
Mode	Router OSPF Config

OSPF Interface Commands

ip ospf area

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 *area-id* [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

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 *kbps*
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

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

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

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

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` *`seconds`*
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

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` *seconds*
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

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

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

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 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	`ip ospf priority` *`priority`*
Mode	Interface Config

no ip ospf priority

This command sets the default OSPF priority for the specified router interface.

Format	`no ip ospf priority`
Mode	Interface Config

ip ospf retransmit-interval

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	`ip ospf retransmit-interval` *second*
Mode	Interface Config

no ip ospf retransmit-interval

This command sets the default OSPF retransmit Interval for the specified interface.

Format	`no ip ospf retransmit-interval`
Mode	Interface Config

ip ospf transmit-delay

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	`ip ospf transmit-delay` *second*
Mode	Interface Config

no ip ospf transmit-delay

This command sets the default OSPF Transit Delay for the specified interface.

Format	`no ip ospf transmit-delay`
Mode	Interface Config

ip ospf mtu-ignore

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	`ip ospf mtu-ignore`
Mode	Interface Config

no ip ospf mtu-ignore

This command enables the OSPF MTU mismatch detection.

Format	`no ip ospf mtu-ignore`
Mode	Interface Config

IP Event Dampening Commands

dampening

Use this command to enable IP event dampening on a routing interface.

Format	`dampening [`*`half-life period`*`] [`*`reuse-threshold suppress-threshold max-suppress-time`*` [restart `*`restart-penalty`*`]]`
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	`no dampening`
Mode	Interface Config

show dampening interface

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

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.
Restart	Configured restart penalty.

Note: The command *clear counters* on page 226 resets the flap count to zero.

Note: The interface CLI command *no shutdown* on page 886 resets the suppressed state to `False`.

Note: Any change in the dampening configuration resets the current penalty, reuse time and suppressed state to their default values, meaning `0`, `0`, and `False` 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
```

OSPF Graceful Restart Commands

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.

The following switches support OSPF graceful restart:

- M6100
- M5300-28G3
- M5300-52G3
- M5300-28GF3

The following switches support OSPF graceful restart with an L3 license:

- M5300-28G
- M5300-52G
- M5300-28G-POE+

- M5300-52G-POE+

nsf (OSPF)

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	OSPF Router Configuration

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

Use this command to disable graceful restart for all restarts.

nsf restart-interval (OSPF)

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` *seconds*
Modes	OSPF Router Configuration

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 nsfrestart-interval

Use this command to revert the grace period to its default value.

Format	`no [ietf] nsf restart-interval`
Modes	OSPF Router Configuration

nsf helper

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	`nsf helper [planned-only]`
Modes	OSPF Router Configuration

Parameter	Description
planned-only	This optional keyword indicates that OSPF should only help a restarting router performing a planned restart.

no nsf helper

Use this command to disable helpful neighbor functionality for OSPF.

Format	`no nsf helper`
Modes	OSPF Router Configuration

nsf ietf helper disable (OSPF)

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	`nsf ietf helper disable`
Modes	OSPF Router Configuration

nsf helper strict-lsa-checking (OSPF)

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	`nsf [ietf] helper strict-lsa-checking`
Modes	OSPF Router Configuration

Parameter	Description
ietf	This keyword is accepted but not required.

no nsf [ietf] helper strict-lsa-checking

Use this command to allow OSPF to continue as a helpful neighbor in spite of topology changes.

Default	Enabled.
Format	`nsf [ietf] helper strict-lsa-checking`
Modes	OSPF Router Configuration

OSPFv2 Stub Router Commands

max-metric router-lsa (OSPFv2 Router Configuration)

To configure OSPF to enter stub router mode, use this command in Router OSPF Global 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 (max-metric router-lsa on-startup), and then enter max-metric router lsa, there is no change. If OSPF is administratively in stub router mode (the max-metric router-lsa command has been given), and you configure OSPF to enter stub router mode on startup (max-metric router-lsa on-startup), OSPF exits stub router mode (assuming the startup period has expired) and the configuration is updated.

Default	`OSPF is not in stub router mode by default`
Format	`max-metric router-lsa [on-startup` *`seconds`*`] [summary-lsa {`*`metric`*`}]`
Mode	OSPFv2 Router Configuration

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 (0xFFFFFF).
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 OSPFv2 Router Configuration 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	`no max-metric router-lsa [on-startup] [summary-lsa]`
Mode	OSPFv2 Router Configuration

clear ip ospf stub-router

Use the clear ip ospf stub-router command in Privileged EXEC mode 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 it if is in stub router mode at startup. This command has no effect if OSPF is configured to be in stub router mode permanently.

Format	`clear ip ospf stub-router`
Mode	Privileged EXEC

OSPF Show Commands

show ip ospf

This command displays information relevant to the OSPF router.

Format	`show ip ospf`
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.
Flood Pacing Interval	The average time, in milliseconds, between LS Update packet transmissions on an interface. This is the value configured with the command *timers pacing flood* on page 759.
LSA Refresh Group Pacing Time	The size in seconds of the LSA refresh group window. This is the value configured with the command *timers pacing lsa-group (OSPF)* on page 759.
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.

Term	Definition
Maximum Paths	The maximum number of paths that OSPF can report for a given 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.
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.

Term	Definition
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 at any given time.
Retransmit Entries High Water Mark	The maximum number of LSAs on all neighbors' retransmit lists at any given time.
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. • 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.

Term	Definition
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.

Command example:

```
(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

This command displays the internal OSPF routing table entries to Area Border Routers (ABR). This command takes no options.

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.
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

This command displays information about the area. The *area-id* identifies the OSPF area that is being displayed.

Format	`show ip ospf area` *area-id*
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 a 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.

Term	Definition
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

This command displays the internal OSPF routing table entries to Autonomous System Boundary Routers (ASBR). This command takes no options.

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

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	`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}]}]]`
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 *`lsid`* can be an IP address or an integer in the range of 0-4294967295.
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

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.
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

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 directly instead of in a *unit/slot/port* format. The *vlan-id* can be a number from 1–4093.

Format	`show ip ospf interface {`*unit/slot/port* `|` `vlan` *vland-id* `|` `loopback` *loopback-id*`}`
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.

Term	Definition
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.
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 *broadcast*. 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 given interface.

Command example:

The following output displays when the OSPF Admin Mode is disabled:

```
(NETGEAR Routing) >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

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	*unit/slot/port*
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.

Term	Definition
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

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 directly instead of in a *unit/slot/port* format. The *vlan-id* can be a number from 1–4093.

Format	`show ip ospf interface stats {`*`unit/slot/port`*` | vlan `*`vland-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.

Term	Definition
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 AllDrRouters 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.
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.

Table 12. Type of OSPF packets 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

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 timers pacing lsa-group) 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

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 or tunnel, only the information for that interface or tunnel 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 directly instead of in a *unit/slot/port* format. 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 {`*unit/slot/port* `|` `vlan` *vland-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.
IP Address	The IP address of the neighbor.
Interface	The interface of the local router in *unit/slot/port* 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 is to decide which router is the master and to decide upon the initial DD sequence number. • 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.
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	*unit/slot/port*
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.

Term	Definition
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.
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 NETGEAR Managed Switch software 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

This command displays the set of OSPFv2 area ranges configured for a given area.

Format	`show ip ospf range` *area-id*
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

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	`show ip ospf statistics`
Modes	Privileged EXEC

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

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

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 752).

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.

Parameter	Description
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.
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

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 ip 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.
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

This command displays the OSPF Virtual Interface information for all areas in the system.

Format	`show ip ospf virtual-link brief`
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.
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.
Transmit Delay	The configured transmit delay for the OSPF virtual interface.

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.

Only the following switches support RIP:

- M6100
- M5300-28G3
- M5300-52G3
- M5300-28GF3

The following switches support RIP with an L3 license:

- M5300-28G
- M5300-52G
- M5300-28G-POE+
- M5300-52G-POE+

router rip

Use this command to enter Router RIP mode.

Format	`router rip`
Mode	Global Config

enable (RIP)

This command resets the default administrative mode of RIP in the router (active).

Default	enabled
Format	`enable`
Mode	Router RIP Config

no enable (RIP)

This command sets the administrative mode of RIP in the router to inactive.

Format	`no enable`
Mode	Router RIP Config

ip rip

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

This command enables the RIP auto-summarization mode.

Default	disabled
Format	`auto-summary`
Mode	Router RIP Config

no auto-summary

This command disables the RIP auto-summarization mode.

Format	`no auto-summary`
Mode	Router RIP Config

default-information originate (RIP)

This command is used to control the advertisement of default routes.

Format	`default-information originate`
Mode	Router RIP Config

no default-information originate (RIP)

This command is used to control the advertisement of default routes.

Format	`no default-information originate`
Mode	Router RIP Config

default-metric (RIP)

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	`default-metric` *metric*
Mode	Router RIP Config

no default-metric (RIP)

This command is used to reset the default metric of distributed routes to its default value.

Format	`no default-metric`
Mode	Router RIP Config

distance rip

This command sets the route preference value of RIP in the router. 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	`distance rip` *preference*
Mode	Router RIP Config

no distance rip

This command sets the default route preference value of RIP in the router.

Format	`no distance rip`
Mode	Router RIP Config

distribute-list out (RIP)

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	`distribute-list` *access-list* `out {ospf | bgp | static | connected}`
Mode	Router RIP Config

no distribute-list out

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	`no distribute-list` *`access list`* `out {ospf | bgp | static | connected}`
Mode	Router RIP Config

ip rip authentication

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	`ip rip authentication {none | {simple` *`key`*`} | {encrypt` *`key keyid`*`}}`
Mode	Interface Config

no ip rip authentication

This command sets the default RIP Version 2 Authentication Type for an interface.

Format	`no ip rip authentication`
Mode	Interface Config

ip rip receive version

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	`ip rip receive version {rip1 | rip2 | both | none}`
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	`no ip rip receive version`
Mode	Interface Config

ip rip send version

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 e only RIP version 1 formatted packets; **`rip2`** for RIP version 2; **`both`** to send packets from either format; 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

This command enables the RIP hostroutesaccept mode.

Default	enabled
Format	`hostroutesaccept`
Mode	Router RIP Config

no hostroutesaccept

This command disables the RIP hostroutesaccept mode.

Format	`no hostroutesaccept`
Mode	Router RIP Config

split-horizon

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

This command sets the default RIP split horizon mode.

Format	`no split-horizon`
Mode	Router RIP Config

redistribute (RIP)

This command configures RIP protocol to redistribute routes from the specified source protocol or routers. Five possible match options exist. When you submit the command **`redistribute ospf match`**, the match option or options that you specify are added to any match types presently being redistributed. Internal routes are redistributed by default. The *`metric`* argument can have a value in the range from 0–15.

Default	metric—not-configured match—internal
Format for OSPF as source protocol	`redistribute ospf [metric` *`metric`*`] [match [[internal] [external 1] [external 2] [nssa-external 1] [nssa-external 2]]`
Format for other source protocols	`redistribute {bgp | static | connected} [metric` *`metric`*`]`
Mode	Router RIP Config

no redistribute

This command deconfigures RIP protocol to redistribute routes from the specified source protocol or routers.

Format	`no redistribute {ospf | bgp | static | connected} [metric] [match [[internal] [external 1] [external 2] [nssa-external 1] [nssa-external 2]]`
Mode	Router RIP Config

show ip rip

This command displays information relevant to the RIP router.

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

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	*`unit/slot/port`*
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

This command displays information related to a particular RIP 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 directly instead of in a *unit/slot/port* format. The *vlan-id* can be a number from 1–4093.

Format	`show ip rip interface {`*unit/slot/port* `| vlan` *vlan-id*`}`
Modes	Privileged EXEC User EXEC

Term	Definition
Interface	*unit/slot/port* This is a configured value.
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 unreachables

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 unreachables`
Mode	Interface Config

no ip unreachables

Use this command to prevent the generation of ICMP Destination Unreachable messages.

Format	`no ip unreachables`
Mode	Interface Config

ip redirects

Use this command to enable the generation of ICMP Redirect messages by the router. 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 router.

Format	`no ip redirects`
Mode	Global Config Interface Config

ipv6 redirects

Use this command to enable the generation of ICMPv6 Redirect messages by the router. 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 router.

Format	`no ipv6 redirects`
Mode	Interface Config

ip icmp echo-reply

Use this command to enable the generation of ICMP Echo Reply messages by the router. 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 router.

Format	`no ip icmp echo-reply`
Mode	Global Config

ip icmp error-interval

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` *`burst-interval`* [*`burst-size`*]
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

11 Captive Portal Commands

This section describes the CLI commands you 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 Commands*
- *Captive Portal 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.

captive-portal

Use this command to enter the Captive Portal Configuration Mode.

Format	`captive-portal`
Mode	Global Config

enable (Captive Portal Config Mode)

This command globally enables the captive portal feature on the switch.

Default	Disable
Format	`enable`
Mode	Captive Portal Config

no enable (Captive Portal Config Mode)

The **`no enable`** command disables the captive portal functionality.

Format	`no enable`
Mode	Captive Portal Config

http port

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	`http port` *`port-number`*
Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch) (Config-CP) #http port 8080
(NETGEAR Switch) (Config-CP) #no http port
```

no http port

This command removes the specified additional HTTP port.

Format	`no http port` *`port-number`*
Mode	Captive Portal Config

https port

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	`https port` *`port-number`*
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

This command set the HTTPS secure port to the default.

Format	`no https port` *`port-number`*
Mode	Captive Portal Config

snmp-server enable traps captive-portal

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

trapflags (Captive Portal Config Mode)

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

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

authentication timeout

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` *`seconds`*
Mode	Captive Portal Config

no authentication timeout

This command sets the authentication timeout to the default value.

Format	`no authentication timeout`
Mode	Captive Portal Config

show captive-portal

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

This command reports status of all captive portal instances in the system.

Format	`show captive-portal status`
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.

Term	Description
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.
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

This command shows which captive portal SNMP traps are enabled.The existing NETGEAR Managed Switch **show trapflags** command shows the global captive portal traps configuration. For more information, see the sample output of *show trapflags* on page 144.

Format	`show captive-portal trapflags`
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)

Use this command to 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	`configuration` *cp-id*
Mode	Captive Portal Config

no configuration

This command deletes a captive portal configuration. The command fails if interfaces are associated to 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	`no configuration` *cp-id*
Mode	Captive Portal Config

enable (Captive Portal Instance)

This command enables a captive portal configuration.

Default	Enable
Format	`enable`
Mode	Captive Portal Instance

no enable

This command disables a captive portal configuration.

Format	`no enable`
Mode	Captive Portal Instance

name

This command configures the name for a captive portal configuration. The *cp-name* can contain up to 32 alphanumeric characters.

Format	`name` *cp-name*
Mode	Captive Portal Instance

protocol

This command configures the protocol mode for a captive portal configuration. The CP can use HTTP or HTTPS protocols.

Default	https
Format	`protocol {http | https}`
Mode	Captive Portal Instance

verification

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

group

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` *`group-id`*
Mode	Captive Portal Instance

radius-auth-server

Use this command to configure a captive portal configuration RADIUS authentication server.

Default	Disable
Format	`radius-auth-server` *`server-name`*
Mode	Captive Portal Instance

no radius-auth-server

This command disables a captive portal configuration RADIUS authentication server.

Format	`no radius-auth-server`
Mode	Captive Portal Instance

redirect-url mode

This command enables the redirect mode for a captive portal configuration.

Default	Disable
Format	`redirect-url mode`
Mode	Captive Portal Instance

no redirect-url mode

This command disables the redirect mode for a captive portal configuration.

Format	`no redirect-url mode`
Mode	Captive Portal Instance

redirect-url

Use this command to specify the URL to which the newly authenticated client is redirected if the URL Redirect Mode is enabled. This command is only available if the redirect mode is enabled.

Format	`redirect-url` *`url`*
Mode	Captive Portal Instance

max-bandwidth-up

This command configures the maximum rate at which a client can send data into the network.

Default	0
Format	`max-bandwidth-up` *`rate`*
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	`no max-bandwidth-up`
Mode	Captive Portal Instance

max-bandwidth-down

This command configures the maximum rate at which a client can receive data from the network.

Default	0
Format	`max-bandwidth-down` *`rate`*
Mode	Captive Portal Instance

Parameter	Description
rate	Rate in bps. 0 indicates 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

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 then the limit is not enforced.

Default	0
Format	`max-input-octets` *bytes*
Mode	Captive Portal Instance

Parameter	Description
bytes	Input octets in bytes. 0 indicates 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

This command configures the maximum number of octets the user is allowed to receive. After this limit has been reached the user will be disconnected. If the value is set to 0 then the limit is not enforced.

Default	0
Format	`max-output-octets` *bytes*
Mode	Captive Portal Commands

Parameter	Description
bytes	Output octets in bytes. 0 indicates 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

This command configures the maximum number of octets the user is allowed to transfer, i.e., the sum of octets transmitted and received. After this limit has been reached the user will be disconnected. If the value is set to 0, then the limit is not enforced.

Default	0
Format	`max-total-octets` *`bytes`*
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)

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` *`timeout`*
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

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	`idle-timeout` *`timeout`*
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	`no idle-timeout`
Mode	Captive Portal Instance

locale

This command is not intended to be a user command. The administrator must use the WEB user interface to create and customize captive portal web content. The command is primarily used by the NETGEAR Managed Switch **`show running config`** command and process as it provides the ability to save and restore configurations using a text-based format.

Format	`locale` *`web-id`*
Mode	Captive Portal Instance

do (Captive Portal Instance mode)

Use this command to run Privileged Exec mode commands.

Format	`do`
Mode	Captive Portal Instance

script-text

Use this command to specify, in UTF-16 byte stream format, the text that is displayed if javascript is disabled in the users browser.

Format	`script-text UTF-16`
Mode	Captive Portal Instance

show (Captive Portal Instance)

Use this command to display the switches options and settings.

Format	`show`
Mode	Captive Portal Instance

wip-msg

Use this command to specify, in UTF-16 byte stream format, the message displayed when authentication is in progress.

Format	`wip-msg UTF-16`
Mode	Captive Portal Instance

interface (Captive Portal Instance)

This command associates an interface to a captive portal configuration or removes the interface captive portal association.

Format	`interface` *`unit/slot/port`*
Mode	Captive Portal Instance

no interface

This command removes the association between an interface and a captive portal configuration.

Format	`no interface` *`unit/slot/port`*
Mode	Captive Portal Instance

block

This command blocks all traffic for a captive portal configuration.

Format	`block`
Mode	Captive Portal Instance

no block

This command unblocks all traffic for a captive portal configuration.

Format	`no block`
Mode	Captive Portal Instance

clear (Captive Portal Instance Config)

This command sets the configuration for this instance to the default values.

Format	`clear`
Mode	Captive Portal Instance

user-logout

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	`user-logout`
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

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` *`color-code`*
Mode	Captive Portal Instance

foreground-color

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` *`color-code`*
Mode	Captive Portal Instance

separator-color

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` *`color-code`*
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

This command displays the operational status of each captive portal configuration. The *`cp-id`* variable is the captive portal ID, which ranges from 1-10.

Format	`show captive-portal configuration` *`cp-id`*
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

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.

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	*unit/slot/port*
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 include the optional *unit/slot/port* information, the following additional information appears:	
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

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	**s**`how 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

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	`show captive-portal configuration` *`cp-id`* `locales`
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

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 [macaddr] 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 slot 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).
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 statistics

This command displays the statistics for a specific captive portal client.

Format	`show captive-portal client macaddr statistics`
Mode	Privileged EXEC

Term	Description
Client MAC Address	Identifies the MAC address of the wireless client (if applicable).
Bytes Received	Total bytes the client has received.
Bytes Transmitted	Total bytes the client has transmitted.

Term	Description
Packets Transmitted	Total packets the client has transmitted.
Packets Received	Total packets the client has received.

show captive-portal interface client status

This command displays information about clients authenticated on all interfaces or a specific interface.

Format	`show captive-portal interface [unit/slot/port] client status`
Mode	Privileged EXEC

Term	Description
Interface	Valid unit, slot and port number.
Interface Description	Describes the interface.
Client MAC Address	Identifies the MAC address of the wireless client (if applicable).
If you use the optional *unit/slot/port* information, the following additional information appears:	
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.
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

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.

Format	`show captive-portal configuration [cp-id] client status`
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.
Client MAC Address	Identifies the MAC address of the wireless client (if applicable).
If you use the optional *cp-id* information, the following additional information appears:	
Client IP Address	Identifies the IP address of the wireless client (if applicable).
Interface	Valid slot and port number separated by a forward slash.
Interface Description	Describes the interface.

captive-portal client deauthenticate

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	`captive-portal client deauthenticate [cp-id] [macaddr]`
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

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	`show captive-portal interface configuration [cp-id] status`
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 slot and port number separated by a forward slash.
Interface Description	Describes the interface.
Type	Shows the type of interface.

show captive-portal interface capability

This command displays all the captive portal eligible interfaces or the interface capabilities for a specific captive portal interface.

Format	`show captive-portal interface capability [`*`unit/slot/port`*`]`
Mode	Privileged EXEC

Field	Description
Interface	Valid slot and port number separated by a forward slash.
Interface Description	Describes the interface.
Type	Shows the type of interface.
If you use the optional *unit/slot/port* information, the following additional information appears:	
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 Commands

Use these commands to view and configure captive portal users in the local database.

user (Captive Portal Config Mode)

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.

Two ways exist to create a user: with the **user name** command or with the **user password** command. If the user is created with the **user name** command, you must assign the password with the **user password** command. If the user is created 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 created a user by using the **user password** command with the user ID and a new password.

Format	user *user-id* name *username*
Mode	Captive Portal Config

Format	user *user-id* password *password*
Mode	Captive Portal Config

Command example:

The following example uses name to create the user.

```
(NETGEAR Switch)(Config-CP) #user 1 name test
```

Command example:

The following example uses password to create the user:

```
(NETGEAR Switch)(Config-CP) #user 1 password test1234
```

no user

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	no user *user-id*
Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch)(Config-CP) #no user 1
```

user name (Captive Portal Config)

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	user *user-id* name *username*
Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch)(Config-CP) #user 1 name johnsmith
```

user password (Captive Portal Config)

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	user *user-id* password *password*
Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch)(Config-CP) #user 1 password
Enter Password (8 - 64 characters):
Re-enter password:
```

user password encrypted

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 *user-id* password encrypted *encrypted-pwd*
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 group (captive portal local user commands)

This command assigns/modifies the group name for the associated captive portal user. The *user-id* variable is the user ID, which is a number in the range of 1 to 128. The *group-name* variable is a name up to 32 characters.

Format	`user` *user-id* `group` *group-name*
Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch)(Config-CP) #user 1 group 123
```

user session-timeout

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 seconds. Use 0 to indicate that the time-out is not enforced.

Default	0
Format	`user` *user-id* `session-timeout` **timeout**
Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch)(Config-CP) #user 1 session-timeout 86400
```

no user session-timeout

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` *user-id* `session-timeout`
Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch)(Config-CP) #no user 1 session-timeout
```

user idle-timeout

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 in seconds. Use 0 to indicate that the time-out is not enforced.

Default	0
Format	`user` *user-id* `idle-timeout` *timeout*
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` *user-id* `idle-timeout`
Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch)(Config-CP) #no user 1 idle-timeout
```

user max-bandwidth-up

This command is used to configure the bandwidth in 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

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

This command is used configure the bandwidth in 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

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` *user-id* `max-bandwidth-down`
Mode	Captive Portal Config

user max-input-octets

This command is used to limit the number of octets in 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` *user-id* `max-input-octets` *octets*
Mode	Captive Portal Config

Parameter	Description
user-id	User ID from 1 to 128 characters.
octets	Number of bytes.

no user max-input-octets

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` *`user-id`* `max-input-octets`
Mode	Captive Portal Config

user max-output-octets

This command is used to limit the number of octets in 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	`user` *`user-id`* `max-output-octets` *`octets`*
Mode	Captive Portal Config

Parameter	Description
user-id	User ID from 1 to 128 characters.
octets	Number of bytes.

no user max-output-octets

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	`no user` *`user-id`* `max-output-octets`
Mode	Captive Portal Config

user max-total-octets

This command is used to limit the number of octets in 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	`user` *user-id* `max-total-octets` *octets*
Mode	Captive Portal Config

Parameter	Description
user-id	User ID from 1 to 128 characters.
octets	Number of bytes.

no user max-total-octets

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` *user-id* `max-total-octets`
Mode	Captive Portal Config

show captive-portal user

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 [`*user-id*`] [group [`*group-id*`]]`
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 *[user-id]* variable, the following information also displays:	

Field	Description
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

This command deletes all captive portal user entries.

Format	`clear captive-portal users`
Mode	Privileged EXEC

Captive Portal User Group Commands

Use the following commands to configure CP user groups.

user group (captive portal user group commands)

Use this command to create a user group. The *`group-id`* variable is a number in the range of 1–10.

Format	`user group` *`group-id`*
Mode	Captive Portal Config

no user group

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` *`group-id`*
Mode	Captive Portal Config

user group name

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	`user group` *group-id* `name` *name*
Mode	Captive Portal Config

user group moveusers

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	`user group` *group-id* `moveusers` *destination-group-id*
Mode	Captive Portal Config

Command example:

```
(NETGEAR Switch)(Config-CP) #user group 2 moveusers 3
```

12 Border Gateway Protocol Commands

This section describes the commands you use to view and configure Border Gateway Protocol (BGP), which is an exterior gateway routing protocol that you use to route traffic between autonomous systems. The BGP CLI commands are available in the NETGEAR Managed Switch software BGP package.

Note: BGP commands are supported on M6100 series switches only.

The chapter contains the following sections:

- *BGP Commands*
- *Routing Policy 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**. Reset part of the protocol state.

BGP Commands

router bgp

This command enables BGP and identifies the autonomous system (AS) number of the router. Only a single instance of BGP can be run and the router can only belong to a single AS.

Default	BGP is inactive by default.
Format	`router bgp as-number`
Mode	Global Config

Parameter	Description
as-number	The router's autonomous system number (ASN).

no router bgp

If you enter the **`no router bgp`** command, BGP is disabled and all BGP configuration reverts to default values. Alternatively, you can use *no enable (BGP)* on page 855 in BGP Router Configuration mode to disable BGP globally without clearing the BGP configuration.

Default	BGP is inactive by default.
Format	`no router bgp as-number`
Mode	Global Config

address-family ipv6

To enter IPv6 Address Family Configuration mode in order to specify IPv6-specific configuration parameters, use the **`address-family ipv6`** command in BGP Router Configuration mode. Commands entered in this mode can be used to enable exchange of IPv6 routes, specify IPv6 prefixes to be originated, and configure inbound and outbound policies to be applied to IPv6 routes.

Default	Exchange of IPv6 routes is disabled by default.
Format	`address-family ipv6`
Mode	BGP Router Config

no address-family ipv6

Use the **no address-family ipv6** command to clear all IPv6 address family configuration.

Format	no address-family ipv6
Mode	BGP Router Config

aggregate-address

To configure a summary address for BGP, use the **aggregate-address** command in Router Configuration mode. No aggregate addresses are configured by default. Unless the options are specified, the aggregate is advertised with the ATOMIC_AGGREGATE attribute and an empty AS path, and the more specific routes are advertised along with the aggregate.

To be considered a match for an aggregate address, a prefix must be more specific (i.e. have a longer prefix length) than the aggregate address. A prefix whose prefix length equals the length of the aggregate address is not considered a match.

When BGP originates a summary address, it installs a reject route in the common routing table for the summary prefix. Any received packets that match the summary prefix, but not a more specific route, match the reject route and are dropped.

BGP accepts up to 128 summary addresses for each address family.

Default	No aggregate addresses are configured by default. Unless the options are specified, the aggregate is advertised with the ATOMIC_AGGREGATE attribute and an empty AS path, and the more specific routes are advertised along with the aggregate.
Format	aggregate-address {*address mask* | *ipv6-prefix/pfx-len*} [as-set] [summary-only]
Mode	BGP Router Config

Parameter	Description
address mask	Summary IPv4 prefix and mask. The default route (0.0.0.0 0.0.0.0) cannot be configured as an aggregate-address. The mask cannot be a 32-bit mask (255.255.255.255). The combination of prefix and mask must be a valid unicast destination prefix.
ipv6-prefix/pfx-len	Summary IPv6 prefix and prefix length. The range for prefix length is 1 to 127.
as-set	(Optional) Normally, the aggregate is advertised with an empty AS path and the ATOMIC_AGGREGATE attribute. If the as-set option is configured, then the aggregate is advertised with a nonempty AS_PATH. If the AS_PATH of all contained routes is the same, then the AS_PATH of the aggregate is the AS_PATH of the contained routes. Otherwise, if the contained routes have different AS_PATHs, the AS_PATH attribute includes an AS_SET with each of the AS numbers listed in the AS PATHs of the aggregated routes. If the as-set option is not configured, the aggregate is advertised with an empty AS_PATH.
summary-only	(Optional) When the summary-only option is given, the more-specific routes within the aggregate address are not advertised to neighbors.

no aggregate-address

Use this command to delete a summary address for BGP. The *address-mask* is a summary prefix and mask.

Format	`no aggregate-address` *address-mask*
Mode	BGP Router Config

bgp aggregate-different-meds (BGP Router Config)

Use the **bgp aggregate-different meds** command in BGP Router Configuration mode to allow the aggregation of routes with different MED attributes. By default, BGP only aggregates routes that have the same MED value, as prescribed by RFC 4271.

When this command is given, the path for an active aggregate address is advertised without a MED attribute. When this command is not given, if multiple routes match an aggregate address, but have different MEDs, the aggregate takes the MED of the first matching route. Any other matching prefix with the same MED is included in the aggregate. Matching prefixes with different MEDs are not considered to be part of the aggregate and continue to be advertised as individual routes.

Default	All the routes aggregated by a given aggregate address must have the same MED value.
Format	`bgp aggregate-different-meds`
Mode	BGP Router Config

no bgp aggregate-different-meds (BGP Router Config)

Use the **no bgp aggregate-different meds** command in BGP Router Configuration mode to return the command to the default.

Format	`no bgp aggregate-different-meds`
Mode	BGP Router Config

bgp aggregate-different-meds (IPv6 Address Family Config)

Use the **bgp aggregate-different meds** command in IPv6 Address Family Configuration mode to allow the aggregation of IPv6 routes with different MED attributes. By default, BGP only aggregates routes that have the same MED value, as prescribed by RFC 4271.

When this command is given, the path for an active aggregate address is advertised without a MED attribute. When this command is not given, if multiple routes match an aggregate address, but have different MEDs, the aggregate takes the MED of the first matching route. Any other matching prefix with the same MED is included in the aggregate. Matching prefixes with different MEDs are not considered to be part of the aggregate and continue to be advertised as individual routes.

Default	All the routes aggregated by a given aggregate address must have the same MED value.
Format	`bgp aggregate-different-meds`
Mode	IPv6 Address Family Config

no bgp aggregate-different-meds

Use the **`no bgp aggregate-different meds`** command in IPv6 Address Family Configuration mode to return the command to the default.

Format	`no bgp aggregate-different-meds`
Mode	IPv6 Address Family Config

bgp always-compare-med (BGP Router Config)

To compare MED values during the decision process in paths received from different ASs, use the bgp always-compare med command in Router Configuration mode. The MED is a 32-bit integer, commonly set by an external peer to indicate the internal distance to a destination. The decision process compares MED values to prefer paths that have a shorter internal distance. Since different ASs may use different internal distance metrics or have different policies for setting the MED, the decision process normally does not compare MED values in paths received from peers in different autonomous systems. This command allows you to force BGP to compare MEDs, regardless of whether paths are received from a common AS.

Default	By default, MED values are only compared for paths received from peers in the same AS.
Format	`bgp always-compare-med`
Mode	BGP Router Config

no bgp always-compare-med

Use the no form of this command to revert to the default behavior, only comparing MED values from paths received from neighbors in the same AS.

Format	`no bgp always-compare-med`
Mode	BGP Router Config

bgp always-compare-med (IPv6 Address Family Config)

To compare MED values during the decision process in paths received from different ASs, use the **`bgp always-compare med`** command in IPv6 Address Family Configuration mode. The MED is a 32-bit integer, commonly set by an external peer to indicate the internal distance to a destination. The decision process compares MED values to prefer paths that have a shorter internal distance. Since different ASs may use different internal distance

metrics or have different policies for setting the MED, the decision process normally does not compare MED values in paths received from peers in different autonomous systems. This command allows you to force BGP to compare MEDs, regardless of whether paths are received from a common AS.

Default	By default, MED values are only compared for paths received from peers in the same AS.
Format	`bgp always-compare-med`
Mode	IPv6 Address Family Config

no bgp always-compare-med

Use the **`no bgp always-compare-med`** command to revert to the default behavior, only comparing MED values from paths received from neighbors in the same AS.

Format	`no bgp always-compare-med`
Mode	IPv6 Address Family Config

bgp client-to-client reflection (BGP Router Config)

By default, a route reflector reflects routes received from its clients to its other clients. However, if a route reflector's clients have a full BGP mesh, the route reflector does not reflect to the clients. The **`bgp client-to-client reflection`** command enables client-to-client reflection for IPv4 routes.

Route reflection can change the routes clients select. A route reflector only reflects those routes it selects as best routes. Best route selection can be influenced by the IGP metric of the route to reach the BGP next hop. Since a client's IGP distance to a given next hop may differ from the route reflector's IGP distance, a route reflector may not readvertise a route a client would have selected as best in the absence of route reflection. One way to avoid this effect is to fully mesh the clients within a cluster. When clients are fully meshed, there is no need for the cluster's route reflectors to reflect client routes to other clients within the cluster. When client-to-client reflection is disabled, a route reflector continues to reflect routes from non-clients to clients and from clients to non-clients.

Note: This command only affects the advertisement of IPv4 routes. The same command is available in Address-Family ipv6 Configuration mode for IPv6 routes.

Default	Client-to-client reflection is enabled when a router is configured as a route reflector.
Format	`bgp client-to-client reflection`
Mode	BGP Router Config

no bgp client-to-client reflection (BGP Router Config)

Use the **no bgp client-to-client reflection** command to disable client-to-client reflection for IPv4 routes.

Note: This command only affects the advertisement of IPv4 routes. The same command is available in Address-Family ipv6 Configuration mode for IPv6 routes.

Format	no bgp client-to-client reflection
Mode	BGP Router Config

bgp client-to-client reflection (IPv6 Address Family Config)

By default, a route reflector reflects routes received from its clients to its other clients. However, if a route reflector's clients have a full BGP mesh, the route reflector does not reflect to the clients. The **bgp client-to-client reflection** command enables client-to-client reflection for IPv6 routes.

Route reflection can change the routes clients select. A route reflector only reflects those routes it selects as best routes. Best route selection can be influenced by the IGP metric of the route to reach the BGP next hop. Since a client's IGP distance to a given next hop may differ from the route reflector's IGP distance, a route reflector may not readvertise a route a client would have selected as best in the absence of route reflection. One way to avoid this effect is to fully mesh the clients within a cluster. When clients are fully meshed, there is no need for the cluster's route reflectors to reflect client routes to other clients within the cluster. When client-to-client reflection is disabled, a route reflector continues to reflect routes from non-clients to clients and from clients to non-clients.

Default	Client-to-client reflection is enabled when a router is configured as a route reflector.
Format	bgp client-to-client reflection
Mode	IPv6 Address Family Config

no bgp client-to-client reflection (IPv6 Address Family Config)

Use the **no bgp client-to-client reflection** command to disable client-to-client reflection for IPv6 routes.

Format	no bgp client-to-client reflection
Mode	IPv6 Address Family Config

bgp cluster-id

Use the **bgp cluster-id** command in BGP router configuration mode to specify the cluster ID of a route reflector. To revert the cluster ID to its default, use the no form of this command.

A route reflector and its clients form a cluster. Since a cluster with a single route reflector has a single point of failure, a cluster may be configured with multiple route reflectors. To avoid sending multiple copies of a route to a client, each route reflector in a cluster should be configured with the same cluster ID. Route reflectors with the same cluster ID must have the same set of clients; otherwise, some routes may not be reflected to some clients. The same cluster ID is used for both IPv4 and IPv6 route reflection.

Default	A route reflector with an unconfigured cluster ID uses its BGP router ID (configured with *bgp router-id*) as the cluster ID.
Format	`bgp cluster-id` *`cluster-id`*
Mode	BGP Router Config

Parameter	Description
cluster-id	A non-zero 32-bit identifier that uniquely identifies a cluster of route reflectors and their clients. The cluster ID may be entered in dotted notation like an IPv4 address or as an integer.

no bgp cluster-id

Use the **no bgp cluster-id** command in BGP router configuration mode to revert the cluster ID to its default.

Format	`no bgp cluster-id`
Mode	BGP Router Config

bgp default local-preference

Use this command to specify the default local preference. Local preference is an attribute sent to internal peers to indicate the degree of preference for a route. A route with a numerically higher local preference value is preferred.

BGP assigns the default local preference to each path received from an external peer. (BGP retains the LOCAL_PREF on paths received from internal peers.) BGP also assigns the default local preference to locally-originated paths. If you change the default local preference, BGP automatically initiates a soft inbound reset for all peers to apply the new local preference.

Default	If this command is not given, BGP advertises a local preference of 100 in Update messages to internal peers.
Format	`bgp default local-preference` *`number`*
Mode	BGP Router Config

Parameter	Description
number	The value to use as the local preference for routes advertised to internal peers. The range is 0 to 4,294,967,295.

no bgp default local-preference

This command sets the default value of local preference of the BGP router.

Format	`no bgp default local-preference`
Mode	BGP Router Config

bgp fast-external-failover

Use this command to configure BGP to immediately reset the adjacency with an external peer if the routing interface to the peer goes down. When BGP gets a routing interface down event, BGP drops the adjacency with all external peers whose IPv4 address is in one of the subnets on the failed interface. This behavior can be overridden for specific interfaces using the command *ip bgp fast-external-failover* on page 855.

Default	Fast external failover is enabled by default.
Format	`bgp fast-external-failover`
Mode	BGP Router Config

no bgp fast-external-failover

Use this command to disable BGP fast-external-failover.

Format	`no bgp fast-external-failover`
Mode	BGP Router Config

bgp fast-internal-failover

Use this command to configure BGP to immediately reset the adjacency with an internal peer when there is a loss of reachability to an internal peer. BGP tracks the reachability of each internal peer’s IP address. If a peer becomes unreachable (that is, the RIB no longer has a nondefault route to the peer’s IP address), then BGP drops the adjacency.

Default	Fast internal failover is enabled by default.
Format	`bgp fast-internal-failover`
Mode	BGP Router Config

no bgp fast-internal-failover

Use this command to return the *bgp fast-internal-failover* command to the default.

Format	`no bgp fast-internal-failover`
Mode	BGP Router Config

bgp log-neighbor-changes

Use this command to enable logging of adjacency state changes. Both backward and forward adjacency state changes are logged. Forward state changes, except for transitions to the Established state, are logged at the Informational severity level. Backward state changes and forward changes to Established are logged at the Notice severity level.

Default	Neighbor state changes are not logged by default.
Format	`bgp log-neighbor-changes`
Mode	BGP Router Config

no bgp log-neighbor-changes

Use this command to return the *bgp log-neighbor-changes* command to the default.

Format	`no bgp log-neighbor-changes`
Mode	BGP Router Config

bgp maxas-limit

To specify a limit on the length of AS Paths that BGP accepts from its neighbors, use the bgp maxas-limit in Router Configuration mode. If BGP receives a path whose AS Path attribute is longer than the configured limit, BGP discards it.

Default	NETGEAR Managed Switch BGP accepts AS paths with up to 75 AS numbers.
Format	`bgp maxas-limit` *`number`*
Mode	BGP Router Config

Parameter	Description
number	The maximum length of an AS Path that BGP will accept from any of its neighbors. The length is the number of autonomous systems listed in the path. The limit may be set to any value from 1 to 100.

no bgp maxas-limit

To revert to the default the limit on the length of AS Paths that BGP accepts from its neighbors, use the no form of this command.

Format	`no bgp maxas-limit`
Mode	BGP Router Config

bgp router-id

Use this command to set the BGP router ID. There is no default BGP router ID. The system does not select a router ID automatically. You must configure one manually.

The BGP router ID must be a valid IPv4 unicast address, but is not required to be an address assigned to the router. The router ID is specified in the dotted notation of an IP address. Setting the router ID to 0.0.0.0 disables BGP. Changing the router ID disables and re-enables BGP, causing all adjacencies to be re-established.

Default	0.0.0.0
Format	`bgp router-id` *`router-id`*
Mode	BGP Router Config

Parameter	Description
router-id	An IPv4 address for BGP to use as its router ID.

no bgp router-id

Use this command to reset the BGP router ID, disabling BGP.

Format	`no bgp router-id router-id`
Mode	BGP Router Config

default-information originate (BGP Router Config)

Use this command to allow BGP to originate a default route. By default, BGP does not originate a default route. If a default route is redistributed into BGP, BGP does not advertise the default route unless the **`default-information originate`** command has been given. The **`always`** option is disabled by default.

Default	BGP does not originate a default route. The **`always`** option is disabled by default.
Format	`default-information originate [always]`
Mode	BGP Router Config

Parameter	Description
always	(Optional) This optional keyword allows BGP to originate a default route, even if the common routing table has no default route.

no default-information originate

Use this command to disable BGP from originating a default route.

Format	`no default-information originate`
Mode	BGP Router Config

default-information originate (IPv6 Address Family Config)

Use this command in IPv6 Address Family Config mode to allow BGP to originate an IPv6 default route. By default, BGP does not originate an IPv6 default route. If an IPv6 default route is redistributed into BGP, BGP does not advertise the IPv6 default route unless the **`default-information originate`** command has been given. The **`always`** option is disabled by default.

Default	BGP does not originate an IPv6 default route. The **`always`** option is disabled by default.
Format	`default-information originate [always]`
Mode	IPv6 Address Family Config

Parameter	Description
always	(Optional) This optional keyword allows BGP to originate an IPv6 default route, even if the common routing table has no IPv6 default route.

no default-information originate (IPv6 Address Family Config)

Use this command to disable BGP from originating an IPv6 default route.

Format	`no default-information originate`
Mode	IPv6 Address Family Config

default metric (BGP Router Config)

Use this command to set the value of the Multi Exit Discriminator (MED) attribute on routes redistributed into BGP when no metric has been specified in the command *redistribute (BGP Router Config)* on page 879.

Default	No default metric is set and no MED is included in redistributed routes.
Format	`default-metric` *`value`*
Mode	BGP Router Config

Parameter	Description
value	The value to set as the MED. The range is 1 to 4,294,967,295.

no default metric (BGP Router Config)

Use this command to delete the default for the metric of redistributed routes.

Format	`no default-metric`
Mode	BGP Router Config

default metric (IPv6 Address Family Config)

Use this command to set the metric of redistributed IPv6 routes when a metric has been configured in the command *redistribute (BGP Router Config)* on page 879.

Default	No default metric is set and no MED is included in redistributed routes.
Format	`default-metric` *`value`*
Mode	IPv6 Address Family Config

Parameter	Description
value	The value to set as the MED. The range is 1 to 4,294,967,295.

no default metric (IPv6 Address Family Config)

Use this command to delete the default for the metric of redistributed IPv6 routes.

Format	`no default-metric`
Mode	IPv6 Address Family Config

distance (BGP Router Config)

Use this command to set the preference (also known as administrative distance) of BGP routes to specific destinations. You may enter up to 128 instances of this command. Two instances of this command may not have the same prefix and wildcard mask. If a distance command is configured that matches an existing distance command's prefix and wildcard mask, the new command replaces the existing command. There can be overlap between the prefix and mask configured for different commands. When there is overlap, the command

whose prefix and wildcard mask are the longest match for a neighbor's address is applied to routes from that neighbor.

An ECMP route's distance is determined by applying distance commands to the neighbor that provided the best path.

The distance command is not applied to existing routes. To apply configuration changes to the distance command itself or the prefix list to which a distance command applies, you must force a hard reset of affected neighbors.

Default	BGP assigns preference values according to the **`distance bgp`** command, unless overridden for specific neighbors or prefixes by this command.
Format	`distance` *`distance`* [*`prefix wildcard-mask`* [*`prefix-list`*]]
Mode	BGP Router Config

Parameter	Description
distance	The preference value for matching routes. The range is 1 to 255.
prefix wildcard-mask	[Optional] Routes learned from BGP peers whose address falls within this prefix are assigned the configured distance value. The wildcard-mask is an inverted network mask whose 1 bits indicate the don't care portion of the prefix.
prefix-list	[Optional] A prefix list can optionally be specified to limit the distance value to a specific set of destination prefixes learned from matching neighbors.

Command example:

The following example sets the preference value of the BGP route to 100.0.0.0/8 from neighbor 10.1.1.1:

```
(R1) (Config)# ip prefix-list pfx-list1 permit 100.0.0.0/8
(R1) (Config)# router bgp 1
(R1) (Config-router)# distance 25 10.1.1.1 0.0.0.0 pfx-list1
```

Command example:

The following example sets the preference value to 12 for all BGP routes from neighbor 10.1.1.1:

```
(R1) (Config-router)# distance 12  10.1.1.1  0.0.0.0
```

Command example:

The following example sets the preference value of all routes within 100.0.0.0/8 from any neighbor:

```
(R1) (Config)# ip prefix-list pfx-list2 permit 100.0.0.0/8 ge 8
(R1) (Config)# router bgp 1
(R1) (Config-router)#distance 25 0.0.0.0 255.255.255.255 pfx-list2
```

no distance (BGP Router Config)

Use this command to set the preference of BGP routes to the default.

Format	`no distance distance [prefix wildcard-mask [prefix-list]]`
Mode	BGP Router Config

distance BGP (BGP Router Config)

Use this command to set the preference, (also known as administrative distance), of BGP routes. Different distance values can be configured for routes learned from external peers, routes learned from internal peers, and BGP routes locally originated. A route with a lower preference value is preferred to a route with a higher preference value to the same destination. Routes with a preference of 255 may not be selected as best routes and used for forwarding.

The change to the default BGP distances does not affect existing routes. To apply a distance change to existing routes, you must force the routes to be deleted from the RIB and relearned, either by resetting the peers from which the routes are learned or by disabling and re-enabling BGP.

Default	external – 20 internal – 200 local – 200
Format	`distance bgp external-distance internal-distance local-distance`
Mode	BGP Router Config

Parameter	Description
external-distance	The preference value for routes learned from external peers. The range is 1 to 255.
internal-distance	The preference value for routes learned from internal peers. The range is 1 to 255.
local-distance	The preference value for locally-originated routes. The range is 1 to 255.

no distance BGP (BGP Router Config)

Use this command to set the default route preference value of BGP routes in the router.

Format	`no distance bgp`
Mode	BGP Router Config

distance BGP (IPv6 Address Family Config)

Use this command to set the preference, (also known as administrative distance), for eBGP, iBGP, and locally-originated BGP IPv6 routes. Different distance values can be configured for routes learned from external peers, routes learned from internal peers, and BGP routes

locally originated. A route with a lower preference value is preferred to a route with a higher preference value to the same destination. Routes with a preference of 255 may not be selected as best routes and used for forwarding.

The change to the default BGP distances does not affect existing routes. To apply a distance change to existing routes, you must force the routes to be deleted from the RIB and relearned, either by resetting the peers from which the routes are learned or by disabling and re-enabling BGP.

Default	external – 20 internal – 200 local – 200
Format	`distance bgp` *`external-distance internal-distance local-distance`*
Mode	IPv6 Address Family Config

Parameter	Description
external-distance	The preference value for routes learned from external peers. The range is 1 to 255.
internal-distance	The preference value for routes learned from internal peers. The range is 1 to 255.
local-distance	The preference value for locally-originated routes. The range is 1 to 255.

no distance BGP (IPv6 Address Family Config)

Use this command to set the default route preference value for eBGP, iBGP, and locally-originated BGP IPv6 routes in the router.

Format	`no distance bgp`
Mode	IPv6 Address Family Config

distribute-list prefix in

Use this command to configure a filter that restricts the routes that BGP accepts from all neighbors based on destination prefix. The distribute list is applied to all routes received from all neighbors. Only routes permitted by the prefix list are accepted. If the command refers to a prefix list that does not exist, the command is accepted and all routes are permitted.

Default	No distribute lists are defined by default.
Format	`distribute-list prefix` *`list-name`* `in`
Mode	BGP Router Config

Parameter	Description
list-name	A prefix list used to filter routes received from all peers based on destination prefix.

no distribute-list prefix in

Use this command to disable a filter that restricts the routes that BGP accepts from all neighbors based on destination prefix.

Format	`no distribute-list prefix` *`list-name`* `in`
Mode	BGP Router Config

distribute-list prefix out (BGP)

Use this command to configure a filter that restricts the advertisement of routes based on destination prefix. Only one instance of this command may be defined for each route source (RIP, OSPF, static, connected). One instance of this command may also be configured as a global filter for outbound prefixes.

If the command refers to a prefix list that does not exist, the command is accepted and all routes are permitted.

When a distribute list is added, changed, or deleted for route redistribution, BGP automatically reconsiders all best routes.

Default	No distribute lists are defined by default.
Format	`distribute-list prefix` *`list-name`* `out [`*`protocol`*` | connected | static]`
Mode	BGP Router Config

Parameter	Description
prefix list-name	A prefix list used to filter routes advertised to neighbors.
protocol, connected, and static	(Optional) When a route source is specified, the distribute list applies to routes redistributed from that source. Only routes that pass the distribute list are redistributed. The protocol value may be either rip or ospf.

no distribute-list prefix out (BGP)

Use this command to reset the **`distribute-list out`** command to the default.

Format	`no distribute-list prefix` *`list-name`* `out [`*`protocol`*` | connected | static]`
Mode	BGP Router Config

enable (BGP)

This command globally enables BGP, while retaining the configuration. BGP is enabled by default once you specify the local AS number with the *router bgp* command and configure a router ID with the *bgp maxas-limit* command. When you disable BGP, BGP retains its configuration. If you invoke the *no router bgp* command, all BGP configuration is reset to the default values.

When BGP is administratively disabled, BGP sends a Notification message to each peer with a Cease error code.

Format	`enable`
Mode	BGP Router Config

no enable (BGP)

This command globally disables the administrative mode of BGP on the system, while retaining the configuration.

Format	`no enable`
Mode	BGP Router Config

ip bgp fast-external-failover

This command configures fast external failover behavior for a specific routing interface.

This command overrides for a specific routing interface the fast external failover behavior configured globally. If **`permit`** is specified, the feature is enabled on the interface, regardless of the global configuration. If **`deny`** is specified, the feature is disabled on the interface, regardless of the global configuration.

Default	Fast external failover is enabled globally by default. There is no interface configuration by default.
Format	`ip bgp fast-external-failover {permit | deny}`
Mode	Interface Config

Parameter	Description
permit	This keyword enables fast external failover on the interface, regardless of the global configuration of the feature.
deny	This keyword disables fast external failover on the interface, regardless of the global configuration of the feature.

no ip bgp fast-external-failover

This command unconfigures the feature on the interface, and the interface uses the global setting.

Format	`no ip bgp fast-external-failover`
Mode	Interface Config

maximum-paths (BGP Router Config)

Use this command to specify the maximum number of next hops BGP may include in an Equal Cost Multipath (ECMP) route derived from paths received from neighbors outside the local autonomous system.

Paths are considered for ECMP when their attributes are the same (local preference, AS path, origin, MED, peer type and IGP distance). When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

Default	BGP uses a single next hop by default
Format	`maximum-paths` *`number-of-paths`*
Mode	BGP Router Config

Parameter	Description
number-of-paths	The maximum number of next hops in a BGP route. The range is from 1 to 32 unless the platform or SDM template further restricts the range.

no maximum-paths (BGP Router Config)

This command resets back to the default the number of next hops BGP may include in an ECMP route.

Format	`no maximum-paths`
Mode	BGP Router Config

maximum-paths (IPv6 Address Family Config)

Use this command to limit the number of Equal Cost Multipath (ECMP) next hops in IPv6 routes from external peers. BGP may include in an ECMP route derived from paths received from neighbors outside the local autonomous system.

Paths are considered for ECMP when their attributes are the same (local preference, AS path, origin, MED, peer type and IGP distance). When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

Default	BGP uses a single next hop by default
Format	`maximum-paths` *`number-of-paths`*
Mode	IPv6 Address Family Config

Parameter	Description
number-of-paths	The maximum number of next hops in a BGP route. The range is from 1 to 32 unless the platform or SDM template further restricts the range.

no maximum-paths (IPv6 Address Family Config)

This command resets back to the default the number of ECMP next hops in IPv6 routes BGP may include in an ECMP route.

Format	`no maximum-paths`
Mode	IPv6 Address Family Config

maximum-paths igbp (BGP Router Config)

Use this command to specify the maximum number of next hops BGP may include in an Equal Cost Multipath (ECMP) route derived from paths received from neighbors within the local autonomous system.

Paths are considered for ECMP when their attributes are the same (local preference, AS path, origin, MED, peer type, and IGP distance). When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

Default	BGP uses a single next hop by default.
Format	`maximum-paths igbp` *`number-of-paths`*
Mode	BGP Router Config

Parameter	Description
number-of-paths	The maximum number of next hops in a BGP router. The range is from 1 to 32 unless the platform or SDM template further restricts the range.

no maximum-paths igbp (BGP Router Config)

Use this command to reset back to the default the number of next hops BGP may include in an ECMP route derived from paths received from neighbors within the local autonomous system.

Format	`no maximum-paths igbp`
Mode	BGP Router Config

maximum-paths igbp (IPv6 Address Family Config)

Use this command to limit the number of ECMP next hops in IPv6 routes from internal peers.

Paths are considered for ECMP when their attributes are the same (local preference, AS path, origin, MED, peer type, and IGP distance). When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

Default	BGP uses a single next hop by default.
Format	`maximum-paths igbp` *`number-of-paths`*
Mode	IPv6 Address Family Config

Parameter	Description
number-of-paths	The maximum number of next hops in a BGP router. The range is from 1 to 32 unless the platform or SDM template further restricts the range.

no maximum-paths igbp (IPv6 Address Family Config)

Use this command to reset back to the default the number of ECMP next hops BGP may include in an ECMP route derived from IPv6 routes received from neighbors within the local autonomous system.

Format	`no maximum-paths igbp`
Mode	IPv6 Address Family Config

neighbor activate

To enable exchange of IPv6 routes with a neighbor, use the neighbor activate command in IPv6 Address Family Configuration mode. The neighbor address must be the same IP address used in the neighbor remote-as command to create the peer.

When IPv6 is enabled or disabled for a neighbor, the adjacency is brought down and restarted to communicate to the change to the peer. You should completely configure IPv6 policy for the peer before activating the peer.

Default	Exchange of IPv6 routes is disabled by default.
Format	`neighbor` *`ipv4-address`* `activate`
Mode	IPv6 Address Family Config

Parameter	Description
ipv4-address	The IPv4 address of a peer.

Command example:

The following example enables the exchange of IPv6 routes with the external peer at 172.20.1.2 and sets the next hop for IPv6 routes sent to that peer:

```
(R1) (Config)# router bgp 1
(R1) (Config-router)# neighbor 172.20.1.2 remote-as 2
(R1) (Config-router)# address-family ipv6
(R1) (Config-router-af)# neighbor 172.20.1.2 activate
```

```
(R1) (Config-router-af)# neighbor 172.20.1.2 route-map SET-V6-NH out
(R1) (Config-router-af)# exit
(R1) (Config-router)# exit
(R1) (Config)# route-map SET-V6-NH permit 10
(R1) (route-map)# set ipv6 next-hop 2001:1:200::1
```

no neighbor activate

Use the no version of the command to disable exchange of IPv6 routes.

Format	`no neighbor` *`ipv4-address`* `activate`
Mode	IPv6 Address Family Config

Parameter	Description
ipv4-address	The IPv4 address of a peer.

neighbor advertisement-interval (BGP Router Config)

Use this command to configure the minimum time that must elapse between advertisements of the same route to a given neighbor. RFC 4271 recommends the interval for internal peers be shorter than the interval for external peers to enable fast convergence within an autonomous system. This value does not limit the rate of route selection, only the rate of route advertisement. If BGP changes the route to a destination multiple times while waiting for the advertisement interval to expire, only the final result is advertised to the neighbor.

NETGEAR Managed Switch BGP enforces the advertisement interval by limiting how often phase 3 of the decision process can run for each update group. The interval applies to withdrawals as well as active advertisements.

Default	30 seconds for external peers 5 seconds for internal peers
Format	`neighbor` *`ip-address`* `advertisement-interval` *`seconds`*
Mode	BGP Router Config

Parameter	Description
ip-address	The neighbor’s IPv4 address.
seconds	The minimum time between route advertisement, in seconds. The range is 0 to 600 seconds.

no neighbor advertisement-interval (BGP Router Config)

Use this command to return to the default the minimum time that must elapse between advertisements of the same route to a given neighbor.

Format	`no neighbor` *`ip-address`* `advertisement-interval`
Mode	BGP Router Config

neighbor advertisement-interval (IPv6 Address Family Config)

In IPv6 Address Family mode, this command controls the time between sending Update messages containing IPv6 routes.

NETGEAR Managed Switch BGP enforces the advertisement interval by limiting how often phase 3 of the decision process can run for each update group. The interval applies to withdrawals as well as active advertisements.

Default	30 seconds for external peers 5 seconds for internal peers
Format	`neighbor` *`ip-address`* `advertisement-interval` *`seconds`*
Mode	IPv6 Address Family Config

Parameter	Description
ip-address	The neighbor's IP address.
seconds	The minimum time between route advertisement, in seconds. The range is 0 to 600 seconds.

no neighbor advertisement-interval (IPv6 Address Family Config)

Use this command to return to the default the minimum time that must elapse between advertisements of the same IPv6 route to a given neighbor.

Format	`no neighbor` *`ip-address`* `advertisement-interval`
Mode	IPv6 Address Family Config

neighbor connect-retry-interval

Use this command in BGP Router Config mode to configure the initial connection retry time for a specific neighbor. If a neighbor does not respond to an initial TCP connection attempt, NETGEAR Managed Switch retries three times. The first retry is after the retry interval configured with neighbor connect-retry-interval. Each subsequent retry doubles the previous retry interval. So by default, the TCP connection is retried after 2, 4, and 8 seconds. If none of the retries is successful, the adjacency is reset to the IDLE state and the IDLE hold timer is started. BGP skips the retries and transitions to IDLE state if TCP returns an error, such as destination unreachable, on a connection attempt.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default	`2 seconds`
Format	`neighbor` *`ip-address`* `connect-retry-interval` *`retry-time`*
Mode	BGP Router Config

Parameter	Description
ip-address	The neighbor's IP address.
retry-time	The number of seconds to wait before attempting to establish a TCP connection with a neighbor after a previous attempt failed.

no neighbor connect-retry-interval

This command resets to the default the initial connection retry time for a specific neighbor.

Format	`no neighbor` *`ip-address`* `connect-retry-interval`
Mode	BGP Router Config

neighbor default-originate (BGP Router Config)

To configure BGP to originate a default route to a specific neighbor, use the **`neighbor default-originate`** command in BGP router configuration mode. By default, a neighbor-specific default has no MED and the Origin is IGP. Attributes may be set using an optional route map. A neighbor-specific default is only advertised if the Adj-RIB-Out does not include a default learned by other means, either from the *default-information originate (BGP Router Config)* command or a default learned from a peer. This type of default origination is not conditioned on the presence of a default route in the routing table. This form of default origination does not install a default route in the BGP routing table (it will not appear in the *show ip bgp* command), nor does it install a default route in the Adj-RIB-Out for the update group of peers so configured (it will not appear in the *show ip bgp neighbors advertised-routes* command).

Origination of the default route is not subject to a prefix filter configured with the command *distribute-list prefix out (BGP)* on page 854.

A route map may be configured to set attributes on the default route sent to the neighbor. If the route map includes a match ip-address term, that term is ignored. If the route map includes match community or match as-path terms, the default route is not advertised. If there is no route map with the route map name given, the default route is not advertised.

Default	No default is originated by default.
Format	`neighbor` *`ip-address`* `default-originate [route-map` *`map-name`*`]`
Mode	BGP Router Config

Parameter	Description
ip-address	The neighbor's IPv4 address.
map-name	(Optional) A route map may be configured to set attributes on the default route advertised to the neighbor.

no neighbor default-originate (BGP Router Config)

Use this command to prevent BGP from originating a default route to a specific neighbor.

Format	`no neighbor` *`ip-address`* `default-originate [route-map` **`map-name`**`]`
Mode	BGP Router Config

neighbor default-originate (IPv6 Address Family Config)

To configure BGP to originate a default IPv6 route to a specific neighbor, use the **`neighbor default-originate`** command in IPv6 Address Family configuration mode. By default, a neighbor-specific default has no MED and the Origin is IGP. Attributes may be set using an optional route map. A neighbor-specific default is only advertised if the Adj-RIB-Out does not include a default learned by other means, either from the *default-information originate (BGP Router Config)* command or a default learned from a peer. This type of default origination is not conditioned on the presence of a default route in the routing table. This form of default origination does not install a default route in the BGP routing table (it will not appear in the *show ip bgp* command), nor does it install a default route in the Adj-RIB-Out for the update group of peers so configured (it will not appear in the *show ip bgp neighbors advertised-routes* command).

Origination of the default route is not subject to a prefix filter configured with the command *distribute-list prefix out (BGP)* on page 854.

A route map may be configured to set attributes on the default route sent to the neighbor. If the route map includes a match ip-address term, that term is ignored. If the route map includes match community or match as-path terms, the default route is not advertised. If there is no route map with the route map name given, the default route is not advertised.

Default	No default is originated by default.
Format	`neighbor` *`ip-address`* `default-originate [route-map` *`map-name`*`]`
Mode	IPv6 Address Family Config

Parameter	Description
ip-address	The neighbor's IPv6 address.
map-name	(Optional) A route map may be configured to set attributes on the default route advertised to the neighbor.

no neighbor default-originate (IPv6 Address Family Config)

Use this command to prevent BGP from originating a default IPv6 route to a specific neighbor.

Format	`no neighbor` *`ip-address`* `default-originate [route-map` *`map-name`*`]`
Mode	IPv6 Address Family Config

neighbor description

Use this command in BGP Router Config mode to record a text description of a neighbor. The description is informational and has no functional impact.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default	No description is originated by default.
Format	`neighbor` *`ip-address`* `description` *`text`*
Mode	BGP Router Config Peer Template Config

Parameter	Description
ip-address	The neighbor's IP address.
text	Text description of neighbor. Up to 80 characters are allowed.

no neighbor description

Use this command to delete the text description of a neighbor.

Format	`no neighbor` *`ip-address`* `description`
Mode	BGP Router Config Peer Template Config

neighbor filter-list (BGP Router Config)

This command filters advertisements to or from a specific neighbor according to the advertisement's AS Path. Only a single AS path list can be configured in each direction for each neighbor. If you invoke the command a second time for a given neighbor, the new AS path list number replaces the previous AS path list number.

If you assign a neighbor filter list to a nonexistent AS path access list, all routes are filtered.

Default	No neighbor filter lists are configured by default.
Format	`neighbor` **`ip-address`** `filter-list` *`as-path-list-number`* `{in | out}`
Mode	BGP Router Config

Parameter	Description
ip-address	The neighbor's IPv4 address.
as-path-list-number	Identifies an AS path list.
in	The AS Path list is applied to advertisements received from the neighbor.
out	The AS Path list is applied to advertisements to be sent to the neighbor.

no neighbor filter-list (BGP Router Config)

Use this command to unconfigure neighbor filter lists.

Format	`no neighbor` *`ip-address`* `filter-list` *`as-path-list-number`* `{in | out}`
Mode	BGP Router Config

neighbor filter-list (IPv6 Address Family Config)

This command filters BGP to apply an AS path access list to UPDATE messages received from or sent to a specific neighbor. Filtering for IPv6 is independent of filtering configured for IPv4. If an UPDATE message includes both IPv4 and IPv6 NLRI, it could be filtered for IPv4 but accepted for IPv6 or vice versa.

If you assign a neighbor filter list to a nonexistent AS path access list, all routes are filtered.

Default	No neighbor filter lists are configured by default.
Format	`neighbor` *`ip-address`* `filter-list` *`as-path-list-number`* `{in | out}`
Mode	IPv6 Address Family Config

Parameter	Description
ip-address	The neighbor's IPv6 address.
as-path-list-number	Identifies an AS path list.
in	The AS Path list is applied to advertisements received from the neighbor.
out	The AS Path list is applied to advertisements to be sent to the neighbor.

no neighbor filter-list (IPv6 Address Family Config)

Use this command to unconfigure neighbor IPv6 filter lists.

Format	`no neighbor` *`ip-address`* `filter-list` *`as-path-list-number`* `{in | out}`
Mode	IPv6 Address Family Config

neighbor inherit peer

To configure a BGP peer to inherit peer configuration parameters from a peer template, use the neighbor inherit peer command in Router Configuration mode. Neighbor session and policy parameters can be configured once in a peer template and inherited by multiple neighbors, eliminating the need to configure the same parameters for each neighbor. Parameters are inherited from the peer template specified and from any templates it inherits from. A neighbor can inherit directly from only one peer template.

Default	`No peer configuration parameters are inherited by default.`
Format	`neighbor` *`ip-address`* `inherit peer` *`template-name`*
Mode	BGP Router Config

Parameter	Description
ip-address	The IP address of a neighbor whose configuration parameters are inherited from the peer template.
template-name	The name of the peer template whose peer configuration parameters are to be inherited by this neighbor.

Command example:

```
(R1) (Config)# router bgp 65000
(R1) (Config-router)# neighbor 172.20.1.2 remote-as 65001
(R1) (Config-router)# neighbor 172.20.2.2 remote-as 65001
(R1) (Config-router)# template peer AGGR
(R1) (Config-rtr-tmp)# timers 3 9
(R1) (Config-rtr-tmp)# address-family ipv4
(R1) (Config-rtr-tmp-af)# send-community
(R1) (Config-rtr-tmp-af)# route-map RM4-IN in
(R1) (Config-rtr-tmp-af)# route-map RM4-OUT out
(R1) (Config-rtr-tmp-af)# exit
(R1) (Config-rtr-tmp)# exit
(R1) (Config-router)# neighbor 172.20.1.2 inherit peer AGGR
(R1) (Config-router)# neighbor 172.20.2.2 inherit peer AGGR
```

no neighbor inherit peer

Use the no neighbor inherit peer command to remove the inheritance.

Format	`no neighbor` *`ip-address`* `inherit peer` *`template-name`*
Mode	BGP Router Config

neighbor maximum-prefix (BGP Router Config)

This command configures the maximum number of prefixes that BGP will accept from a specified neighbor. The prefix limit is compared against the number of prefixes received from the neighbor, including prefixes that are rejected by inbound policy. If the peering session is shut down, the adjacency stays down until the *clear ip bgp* command is issued for the neighbor. The neighbor can also be brought back up using the *neighbor shutdown* command followed by the command *no neighbor shutdown* .

Default	By default the prefix limit is set to the maximum number of routes that can be installed in the forwarding table. The default warning threshold is 75%. A neighbor that exceeds the limit is shutdown unless the **`warning-only`** option is configured.
Format	`neighbor` *`ip-address`* `maximum-prefix {`*`maximum`* `| unlimited} [`*`threshold`*`] [warning-only]`
Mode	BGP Router Config

Parameter	Description
ip-address	The neighbor's IPv4 address.
maximum	The maximum number of prefixes BGP will accept from this neighbor. Range is 0 to the maximum number of routes the router supports.
unlimited	Do not enforce any prefix limit.
threshold	(Optional) When the number of prefixes received from the neighbor exceeds this percentage of the maximum, BGP writes a log message. The range is 1 to 100 percent. The default is 75%.
warning-only	(Optional) If BGP receives more than the maximum number of prefixes, BGP discards excess prefixes and writes a log message rather than shutting down the adjacency.

no neighbor maximum-prefix (BGP Router Config)

This command reverts to the default value for the maximum the number of prefixes that BGP will accept from a specified neighbor.

Format	`no neighbor` *`ip-address`* `maximum-prefix`
Mode	BGP Router Config

neighbor maximum-prefix (IPv6 Address Family Config)

This command specifies the maximum number of IPv6 prefixes that BGP will accept from a specified neighbor. The prefix limit is compared against the number of prefixes received from the neighbor, including prefixes that are rejected by inbound policy. If the peering session is shut down, the adjacency stays down until the *clear ip bgp* command is issued for the neighbor. The neighbor can also be brought back up using the *neighbor shutdown* command followed by the command *no neighbor shutdown*.

Default	By default the prefix limit is set to the maximum number of routes that can be installed in the forwarding table. The default warning threshold is 75%. A neighbor that exceeds the limit is shutdown unless the **warning-only** option is configured.
Format	neighbor *ip-address* maximum-prefix {*maximum* | unlimited [*threshold*] [warning-only]
Mode	IPv6 Address Family Config

Parameter	Description
ip-address	The neighbor's IPv6 address.
maximum	The maximum number of prefixes BGP will accept from this neighbor. Range is 0 to the maximum number of routes the router supports.
unlimited	Do not enforce any prefix limit.
threshold	(Optional) When the number of prefixes received from the neighbor exceeds this percentage of the maximum, BGP writes a log message. The range is 1 to 100 percent. The default is 75%.
warning-only	(Optional) If BGP receives more than the maximum number of prefixes, BGP discards excess prefixes and writes a log message rather than shutting down the adjacency.

no neighbor maximum-prefix (IPv6 Address Family Config)

This command reverts to the default value for the maximum the number of prefixes that BGP will accept from a specified neighbor.

Format	no neighbor *ip-address* maximum-prefix
Mode	IPv6 Address Family Config

neighbor next-hop-self (BGP Router Config)

This command configures BGP to set the next hop attribute to a local IP address when advertising a route to an internal peer. Normally, BGP would retain the next hop attribute received from the external peer.

When the next hop attribute in routes from external peers is retained, internal peers must have a route to the external peer's IP address. This is commonly done by configuring the IGP on the border router to advertise the external (or DMZ) subnet. The next-hop-self option eliminates the need to advertise the external subnet in the IGP.

Default	not enabled
Format	neighbor *ip-address* next-hop-self
Mode	BGP Router Config

Parameter	Description
ip-address	The neighbor's IP address.

no neighbor next-hop-self (BGP Router Config)

This command disables the peer as the next hop for the locally originated paths. After executing this command, the BGP peer must be reset before the changes take effect.

Format	`no neighbor` *`ip-address`* `next-hop-self`
Mode	BGP Router Config

neighbor next-hop-self (IPv6 Address Family Config)

This command configures BGP to use a local address as the IPv6 next hop when advertising IPv6 routes to a specific peer. For IPv6, BGP uses an IPv6 address from the local interface that terminates the IPv4 peering session.

Default	not enabled
Format	`neighbor` *`ip-address`* `next-hop-self`
Mode	IPv6 Address Family Config

Parameter	Description
ip-address	The neighbor's IP address.

no neighbor next-hop-self (IPv6 Address Family Config)

This command disables the peer as the next hop for the locally originated paths. After executing this command, the BGP peer must be reset before the changes take effect.

Format	`no neighbor` *`ip-address`* `next-hop-self`
Mode	IPv6 Address Family Config

neighbor password

Use this command in BGP Router Config mode to enable MD5 authentication of TCP segments sent to and received from a neighbor, and configures an authentication key.

MD5 must either be enabled or disabled on both peers. The same password must be configured on both peers. After a TCP connection is established, if the password on one end is changed, then the password on the other end must be changed to match before the hold time expires. With default hold times, both passwords must be changed within 120 seconds to guarantee the connection is not dropped.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default	`MD5 authentication is disabled.`
Format	`neighbor` *`ip-address`* `password` *`string`*
Mode	BGP Router Config Peer Template Config

Parameter	Description
ip-address	The neighbor's IP address.
string	Case-sensitive password from 1 to 25 characters in length.

no neighbor password

This command disables MD5 authentication of TCP segments sent to and received from a neighbor.

Format	`no neighbor` *`ip-address`* `password`
Mode	BGP Router Config

neighbor prefix-list

This command filters advertisements sent to a specific neighbor based on the destination prefix of each route. Only one prefix list may be defined for each neighbor in each direction. If you assign a prefix list that does not exist, all prefixes are permitted.

Default	No prefix list is configured.
Format	`neighbor` *`ip-address`* `prefix-list` *`prefix-list-name`* `{in | out}`
Mode	BGP Router Config

Parameter	Description
ip-address	The neighbor's IP address.
prefix-list-name	The name of an IP prefix list.
in	Apply the prefix list to advertisements received from this neighbor.
out	Apply the prefix list to advertisements to be sent to this neighbor.

no neighbor prefix-list

This command disables filtering advertisements sent to a specific neighbor based on the destination prefix of each route.

Format	`no neighbor` *`ip-address`* `prefix-list` *`prefix-list-name`* `{in | out}`
Mode	BGP Router Config

neighbor remote-as

This command configures a neighbor and identifies the neighbor's autonomous system. The neighbor's AS number must be specified when the neighbor is created. Up to 128 neighbors may be configured.

Note: The switch does not support a **`remote-as`** *`as-number`* command in Peer Template Configuration mode. You must specify the neighbor's AS number when the neighbor is created.

Default	No neighbors are configured.
Format	`neighbor {`*`ip-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`]} remote-as` *`as number`*
Mode	BGP Router Config

Parameter	Description
ip-address	The neighbor's IP address. For external peers, this address must be an IP address on the link that connects the two peers. For internal peers, the neighbor address can be any address, such as the IP address on a loopback interface. If the neighbor address is an IPv6 link local address, the interface to the neighbor must be specified using the **`neighbor update-source`** command and the IPv6 NEXT_HOP must be explicitly set using the **`set ipv6 next-hop`** command in a route map applied to outbound advertisements to the neighbor.
ipv6-address	The neighbor's IPv6 address. If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
as-number	The autonomous system number of the neighbor's AS. The range is 1 to 65,535. If the neighbor's AS number is the same as the local router, the peer is an internal peer. Otherwise, the peer is an external peer.

no neighbor remote-as

This command unconfigures neighbors.

Format	`no neighbor {`*`ip-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`]} remote-as`
Mode	BGP Router Config

neighbor remove-private-as (BGP Router Config)

Use this command in BGP Router Config mode to remove private AS numbers when advertising IPv4 routes to an external peer.

This command can only be applied to external peers. Private AS numbers are removed or replaced whether or not the original AS path includes any non-private AS numbers. The AS path advertised to the external peer always includes at least one instance of the local AS number; therefore, removing private AS numbers never results in advertisement of an empty AS_PATH attribute. AS numbers from 64512 to 65535 inclusive are considered private. Although 65535 is a reserved ASN and not technically part of the private range, it is treated as a private ASN when removing or replacing private ASNs.

Default	Private AS numbers are not removed by default.
Format	`neighbor` *`ip-address`* `remove-private-as [all replace-as]`
Mode	BGP Router Config

Parameter	Description
ip-address	The neighbor's IPv4 address.
all replace-as	To retain the original AS path length, replace each private AS number with the local AS number. This is optional.

no neighbor remove-private-as

Use this command in BGP Router Config mode to stop removing private AS numbers

Format	`no neighbor` *`ip-address`* `remove-private-as`
Mode	BGP Router Config

neighbor remove-private-as (IPv6 Address Family Config)

Use this command in IPv6 Address Family Config mode to remove private AS numbers when advertising IPv6 routes to an external peer.

This command can only be applied to external peers. Private AS numbers are removed or replaced whether or not the original AS path includes any non-private AS numbers. The AS path advertised to the external peer always includes at least one instance of the local AS number; therefore, removing private AS numbers never results in advertisement of an empty AS_PATH attribute. AS numbers from 64512 to 65535 inclusive are considered private. Although 65535 is a reserved ASN and not technically part of the private range, it is treated as a private ASN when removing or replacing private ASNs.

Default	Private AS numbers are not removed by default.
Format	`neighbor` *`ip-address`* `remove-private-as [all replace-as]`
Mode	IPv6 Address Family Config

Parameter	Description
ip-address	The neighbor's IPv4 or IPv6 address.
all replace-as	To retain the original AS path length, replace each private AS number with the local AS number. This is optional.

no neighbor remove-private-as (IPv6 Address Family Config)

Use this command in IPv6 Address Family Config mode to stop removing private AS numbers when advertising IPv6 routes to an external peer.

Format	`no neighbor` *`ip-address`* `remove-private-as`
Mode	IPv6 Address Family Config

neighbor route-map (BGP Router Config)

To apply a route map to incoming or outgoing routes for a specific neighbor, use the **`neighbor route-map`** command in BGP Router Configur mode. A route map can be used to change the local preference, MED, or AS Path of a route. Routes can be selected for filtering or modification using an AS path access list or a prefix list.

Default	No route maps are applied by default.
Format	`neighbor` *`ip-address`* `route-map` *`map-name`* `{in | out}`
Mode	BGP Router Config

Parameter	Description
ip-address	The neighbor's IP address.
map-name	The name of the route map to be applied.
in or out	Whether the route map is applied to incoming or outgoing routes.

no neighbor route-map (BGP Router Config)

Use the no neighbor route-map command in BGP Router Config mode to remove the route map.

Format	`no neighbor` *`ip-address`* `route-map` *`map-name`* `{in | out}`
Mode	BGP Router Config

neighbor route-map (IPv6 Address Family Config)

Use this command in IPv6 Address Family Config mode to specify a route map to be applied to inbound or outbound IPv6 routes.

Default	No route maps are applied by default.
Format	`neighbor` *`ip-address`* `route-map` *`map-name`* `{in | out}`
Mode	IPv6 Address Family Config

Parameter	Description
ip-address	The neighbor's IP address.
map-name	The name of the route map to be applied.
in or out	Whether the route map is applied to incoming or outgoing routes.

no neighbor route-map (IPv6 Address Family Config)

Use the no neighbor route-map command in IPv6 Address Family Config mode to remove the route map for IPv6 routes.

Format	`no neighbor` *`ip-address`* `route-map` *`map-name`* `{in | out}`
Mode	IPv6 Address Family Config

neighbor route-reflector-client (BGP Router Config)

Use this command in address family or BGP Router Config mode to configure an internal peer as an IPv4 route reflector client.

Normally, a router does not readvertise BGP routes received from an internal peer to other internal peers. If you configure a peer as a route reflector client, this router readvertises such routes. A router is a route reflector if it has one or more route reflector clients. Configuring the first route reflector client automatically makes the router a route reflector.

If you configure multiple route reflectors within a cluster, you must configure each route reflector in the cluster with the same cluster ID. Use the *bgp cluster-id* command to configure a cluster ID.

An external peer may not be configured as a route reflector client.

When reflecting a route, BGP ignores the set statements in an outbound route map to avoid causing the receiver to compute routes that are inconsistent with other routers in the AS.

Default	Peers are not route reflector clients.
Format	`neighbor` *`ip-address`* `route-reflector-client`
Mode	BGP Router Config

Parameter	Description
ip-address	The neighbor's IPv4 address.

no neighbor route-reflector-client

Use this command in BGP Router Config mode to unconfigure an internal peer as an IPv4 route reflector client.

Format	`no neighbor` *`ip-address`* `route-reflector-client`
Mode	BGP Router Config

neighbor route-reflector-client (IPv6 Address Family Config)

Use this command in IPv6 Address Family Config mode to configure an internal peer as an IPv6 route reflector client.

Normally, a router does not readvertise BGP routes received from an internal peer to other internal peers. If you configure a peer as a route reflector client, this router readvertises such routes. A router is a route reflector if it has one or more route reflector clients. Configuring the first route reflector client automatically makes the router a route reflector.

If you configure multiple route reflectors within a cluster, you must configure each route reflector in the cluster with the same cluster ID. Use the *bgp cluster-id* command to configure a cluster ID.

An external peer may not be configured as a route reflector client.

When reflecting a route, BGP ignores the set statements in an outbound route map to avoid causing the receiver to compute routes that are inconsistent with other routers in the AS.

Default	Peers are not route reflector clients.
Format	`neighbor` *`ip-address`* `route-reflector-client`
Mode	IPv6 Address Family Config

Parameter	Description
ip-address	The neighbor’s IPv4 or IPv6 address.

no neighbor route-reflector-client (IPv6 Address Family Config)

Use this command in IPv6 Address Family Config mode to unconfigure an internal peer as an IPv6 route reflector client.

Format	`no neighbor` *`ip-address`* `route-reflector-client`
Mode	IPv6 Address Family Config

neighbor send-community

To configure the local router to send the BGP community attributes in Update messages to a specific neighbor, use the **`neighbor send-community`** command in BGP Router Config mode or IPv6 Address Family Config mode.

Default	The communities attribute is not sent to neighbors by default.
Format	`neighbor` *`ip-address`* `send-community`
Mode	BGP Router Config IPv6 Address Family Config

Parameter	Description
ip-address	The neighbor's IP address.

no neighbor send-community

Use this command in BGP Router Config mode or IPv6 Address Family Config mode to return the community attributes to the default configuration.

Format	`no neighbor` *`ip-address`* `send-community`
Mode	BGP Router Config IPv6 Address Family Config

neighbor shutdown

Use this command in BGP Router Config mode to bring down the adjacency with a specific neighbor. If the adjacency is up when the command is given, the peering session is dropped and all route information learned from the neighbor is purged.

When a neighbor is shut down, BGP first sends a NOTIFICATION message with a Cease error code. When an adjacency is administratively shut down, the adjacency stays down until administratively re-enabled (using the command *no neighbor shutdown* below).

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default	Neighbors are not shutdown by default.
Format	`neighbor` *`ip-address`* `shutdown`
Mode	BGP Router Config Peer Template Config

Parameter	Description
ip-address	The neighbor's IP address. This is the IP address on the link that connects the two peers.

no neighbor shutdown

This command administratively enables a BGP peer.

Format	`no neighbor` *`ip-address`* `shutdown`
Mode	• BGP Router Config • Peer Template Config

neighbor timers

Use this command in BGP Router Config mode to override the global timer values and set the keepalive and hold timers for a specific neighbor. The new values are not applied to adjacencies already in the ESTABLISHED state. A new keepalive or hold time is applied the next time an adjacency is formed.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default	The keepalive and hold timers default to the globally configured values set with the *address-family* command.
Format	`neighbor` *`ip-address`* `timers` *`keepalive holdtime`*
Mode	BGP Router Config Peer Template Config

Parameter	Description
ip-address	The neighbor's IP address. This is the IP address on the link that connects the two peers.
keepalive	The time, in seconds, between BGP KEEPALIVE packets sent to a neighbor. The range is 0 to 65,535 seconds. Jitter is applied to the keepalive interval.
holdtime	The time, in seconds, that BGP continues to consider a neighbor to be alive without receiving a BGP KEEPALIVE or UPDATE packet from the neighbor. If no KEEPALIVE is received from a neighbor for longer than the hold time, BGP drops the adjacency. If the hold time is set to 0, then BGP does not enforce a hold time and BGP does not send periodic KEEPALIVE messages. The range is 0 to 65,535 seconds.

no neighbor timers

This command reverts the keep alive and hold time for a peer to their defaults. After executing this command, the BGP peer must be reset before the changes will take effect.

Format	`no neighbor` *`ip-address`* `timers`
Mode	BGP Router Config

neighbor update-source

Use this command in BGP Router Config mode to configure BGP to use a specific IP address as the source address for the TCP connection with a neighbor. This IP address must be the IP address configured on the peer as its neighbor address for this router.

The IP address used as the source address in IP packets sent to a neighbor must be the same address used to configure the local system as a neighbor of the neighbor router. In other words, if the update source is configured, it must be the same IP address used in the neighbor remote-as command on the peer.

It is common to use an IP address on a loopback interface because a loopback interface is always reachable, as long as any routing interface is up. The peering session can stay up as long as the loopback interface remains reachable. If you use an IP address on a routing interface, then the peering session will go down if that routing interface goes down.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default	When no update source is configured, TCP connections use the primary IPv4 address on the outgoing interface to the neighbor.
Format	`neighbor` *`ip-address`* `update-source` *`interface`*
Mode	BGP Router Config Peer Template Config

Parameter	Description
ip-address	The neighbor's IP address. This is the IP address on the link that connects the two peers.
interface	The primary IPv4 address on this interface is used as the source IP address for the TCP connection with the neighbor.

no neighbor update-source

This command configures BGP to use the primary IPv4 address on the outgoing interface to the neighbor for the TCP connection.

Format	`no neighbor` *`ip-address`* `update-source`
Mode	BGP Router Config Peer Template Config

network (BGP Router Config)

This command configures BGP to advertise an address prefix.The prefix is only advertised if the common routing table includes a nonBGP route with the same prefix. The route may be a connected route, a static route, or a dynamic route from another routing protocol.

BGP accepts up to 64 networks per address family. The network command may specify a default route (network 0.0.0.0 mask 0.0.0.0).

If a route map is configured to set attributes on the advertised routes, match as-path and match community terms in the route map are ignored. A match ip-address prefix-list term is honored in this context. If your route map includes such a match term, the network is only advertised if the prefix list permits the network prefix. If there is no route map with the name given, the network is not advertised.

Default	No networks are advertised by default.
Format	`network` *`prefix`* `mask` *`network-mask`* `[route-map` *`rm-name`*`]`
Mode	BGP Router Config

Parameter	Description
prefix	An IPv4 address prefix in dotted notation.
network-mask	The network mask for the prefix in dotted quad notation (e.g., 255.255.0.0).
rm-name	(Optional) A route map can be used to set path attributes on the route.

no network (BGP Router Config)

This command disables BGP from advertising an address prefix.

Format	`no network` *`prefix`* `mask` *`network-mask`* `[route-map` *`rm-name`*`]`
Mode	BGP Router Config

network (IPv6 Address Family Config)

This command identifies network IPv6 prefixes that BGP originates in route advertisements to its neighbors. The prefix is only advertised if the common routing table includes a non-BGP route with the same prefix. The route may be a connected route, a static route, or a dynamic route from another routing protocol.

BGP accepts up to 64 networks per address family. The network command may specify a default route (network 0.0.0.0 mask 0.0.0.0).

If a route map is configured to set attributes on the advertised routes, match as-path and match community terms in the route map are ignored. A match ip-address prefix-list term is honored in this context. If your route map includes such a match term, the network is only advertised if the prefix list permits the network prefix. If there is no route map with the name given, the network is not advertised.

Default	No networks are advertised by default.
Format	`network` *`ipv6-address/prefix-length`* `[route-map` *`rm-name`*`]`
Mode	IPv6 Address Family Config

Parameter	Description
ipv6-address	Network IPv6 prefixes.
prefix	An IPv4 address prefix in dotted notation.
rm-name	(Optional) A route map can be used to set path attributes on the route.

no network (IPv6 Address Family Config)

This command disables BGP from advertising an address prefix.

Format	`no network` *`ipv6-address/prefix-length`* `[route-map` *`rm-name`*`]`
Mode	IPv6 Address Family Config

redistribute (BGP Router Config)

This command configures BGP to advertise routes learned by means outside of BGP. BGP can redistribute local (connected), static, OSPF, and RIP routes.

The distribute-list out command can also be used to filter redistributed routes by prefix. Either a redistribute route map or a distribute list may be configured, but not both.

A default route cannot be redistributed unless the *default-information originate (BGP Router Config)* command is given.

If a route map is configured, match as-path and match community terms are ignored. If no route map is configured with the name given, no prefixes are redistributed.

Default	BGP redistributes no routes by default. When BGP redistributes OSPF routes, it redistributes only internal routes unless the **`match`** option specifies external routes.
Format	`redistribute {ospf | rip | connected | static} [metric` *`metric-value`*`] [match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-map` *`map-tag`*`]`
Mode	BGP Router Config

Parameter	Description
ospf, rip, connected, static	A source of routes to redistribute.
metric *`metric-value`*	(Optional) When this option is specified, BGP advertises the prefix with the Multi Exit Discriminator path attribute set to the configured value. If this option is not specified, but a default metric is configured for BGP (*default-information originate (IPv6 Address Family Config)* command), then the MED is set to the default metric. If a default metric is not configured, then the prefix is advertised without a MED attribute.

Parameter	Description
match	(Optional) If you configure BGP to redistribute OSPF routes, BGP by default only redistributes internal routes (OSPF intra-area and inter-area routes). Use the **match** option to configure BGP to also redistribute specific types of external routes, or to disable redistribution of internal OSPF routes.
route-map *map-tag*	(Optional) A route map can be used to filter redistributed routes by destination prefix using a prefix list. A route map can be used to set attributes on redistributed routes.

no redistribute (BGP Router Config)

This command removes the configuration for the redistribution for BGP protocol from the specified source protocol/routers. The command **no redistribute opsf match external 1** withdraws only OSPF external type 1 routes, OSPF internal routes are still redistributed.

Format	`no redistribute {ospf | rip | connected | static} [metric` *`metric-value`*`] [match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-map` *`map-tag`*`]`
Mode	BGP Router Config

redistribute (IPv6 Address Family Config)

This command configures BGP to non-BGP routes from the IPv6 routing table. NETGEAR Managed Switch software does not support RIP for IPv6.

The distribute-list out command can also be used to filter redistributed routes by prefix. Either a redistribute route map or a distribute list may be configured, but not both.

A default route cannot be redistributed unless the *default-information originate (BGP Router Config)* command is given.

If a route map is configured, match as-path and match community terms are ignored. If no route map is configured with the name given, no prefixes are redistributed.

Default	BGP redistributes no routes by default. When BGP redistributes OSPF routes, it redistributes only internal routes unless the **match** option specifies external routes.
Format	`redistribute {ospf | connected | static} [metric` *`metric-value`*`] [match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-map` *`map-tag`*`]`
Mode	IPv6 Address Family Config

Parameter	Description
ospf, connected, static	A source of routes to redistribute.
metric *metric-value*	(Optional) When this option is specified, BGP advertises the prefix with the Multi Exit Discriminator path attribute set to the configured value. If this option is not specified, but a default metric is configured for BGP (*default-information originate (IPv6 Address Family Config)* command), then the MED is set to the default metric. If a default metric is not configured, then the prefix is advertised without a MED attribute.
match	(Optional) If you configure BGP to redistribute OSPF routes, BGP by default only redistributes internal routes (OSPF intra-area and inter-area routes). Use the **match** option to configure BGP to also redistribute specific types of external routes, or to disable redistribution of internal OSPF routes.
route-map *map-tag*	(Optional) A route map can be used to filter redistributed routes by destination prefix using a prefix list. A route map can be used to set attributes on redistributed routes.

no redistribute (IPv6 Address Family Config)

This command removes the configuration for the redistribution for BGP protocol from the specified source protocol or routers. For example, the command **no redistribute opsf match external 1** withdraws only OSPF external type 1 routes, OSPF internal routes are still redistributed.

Format	no redistribute {ospf | connected | static} [metric *metric-value*] [match {internal | *external 1* | *external 2* | *nssa-external 1* | *nssa-external 2*}] [route-map *map-tag*]
Mode	IPv6 Address Family Config

template peer

To create a BGP peer template and enter Peer Template Configuration mode, use the **template peer** command in Router Configuration mode. A peer template can be configured with parameters that apply to many peers. Neighbors can then be configured to inherit parameters from the peer template. A peer template can include both session parameters and peer policies. Peer policies are configured with an address family configuration mode and apply only to that address family. You can configure up to 32 peer templates. When you make a change to a template, the change is immediately applied to all neighbors that inherit from the template (although policy changes are subject to a three-minute delay).

Note: NETGEAR Managed Switch does not support a **remote-as** *as-number* command in Peer Template Configuration mode. The neighbor's AS number must be specified when the neighbor is created.

Default	No peer templates are configured by default.
Format	`template peer` *name*
Mode	BGP Router Config

Parameter	Description
name	The name of the template. The name may be no more than 32 characters.

Command example:

```
(R1) (Config)# router bgp 65000
(R1) (Config-router)# neighbor 172.20.1.2 remote-as 65001
(R1) (Config-router)# neighbor 172.20.2.2 remote-as 65001
(R1) (Config-router)# template peer AGGR
(R1) (Config-rtr-tmplt)# timers 3 9
(R1) (Config-rtr-tmplt)# address-family ipv4
(R1) (Config-rtr-tmplt-af)# send-community
(R1) (Config-rtr-tmplt-af)# route-map RM4-IN in
(R1) (Config-rtr-tmplt-af)# route-map RM4-OUT out
(R1) (Config-rtr-tmplt-af)# exit
(R1) (Config-rtr-tmplt)# address-family ipv6
(R1) (Config-rtr-tmplt-af)# send-community
(R1) (Config-rtr-tmplt-af)# route-map RM6-IN in
(R1) (Config-rtr-tmplt-af)# route-map RM6-OUT out
(R1) (Config-rtr-tmplt-af)# exit
(R1) (Config-rtr-tmplt)# exit
(R1) (Config-router)# neighbor 172.20.1.2 inherit peer AGGR
(R1) (Config-router)# neighbor 172.20.2.2 inherit peer AGGR
(R1) (Config-router)# address-family ipv6
(R1) (Config-router)# neighbor 172.20.1.2 activate
(R1) (Config-router)# neighbor 172.20.2.2 activate
```

no template peer

Use the no form of the command to delete a peer template.

Format	`no template peer` *name*
Mode	BGP Router Config

Parameter	Description
name	The name of the template. The name may be no more than 32 characters.

address-family

To configure policy parameters within a peer template to be applied to a specific address family, use the **address-family** command in Peer Template Configuration mode. This command enters an Address Family Configuration mode within the peer template. Policy commands configured within this mode apply to the address family. The following commands can be added to a peer template in Address Family Configuration mode:

- **activate**
- **advertisement-interval** *seconds*
- **default-originate**
- **filter-list** *as-path-list-number* **{in | out}**
- **maximum-prefix {***maximum* **| unlimited} [***threshold***]**
- **next-hop-self**
- **prefix-list** *prefix-list-name* **{in | out}**
- **remove-private-as [all replace-as]**
- **route-map** *map-name* **{in | out}**
- **route-reflector-client**
- **send-community**

Format	`address-family {ipv4 | ipv6}`
Mode	Peer Template Config

Parameter	Description
ipv4	Configure policy parameters for IPv4 routes.
ipv6	Configure policy parameters for IPv6 routes.

Command example:

In the following example, the peer template AGGR sets the keepalive timer to 3 seconds, the hold timer to 9 seconds, allows communities to be sent for both IPv4 and IPv6 routes, and configures different inbound and outbound route maps for IPv4 and IPv6. Two neighbors, 172.20.1.2 and 172.20.2.2, inherit these parameters from the template.

```
(R1) (Config)# router bgp 65000
(R1) (Config-router)# neighbor 172.20.1.2 remote-as 65001
(R1) (Config-router)# neighbor 172.20.2.2 remote-as 65001
(R1) (Config-router)# template peer AGGR
(R1) (Config-rtr-tmplt)# timers 3 9
(R1) (Config-rtr-tmplt)# address-family ipv4
(R1) (Config-rtr-tmplt-af)# send-community
(R1) (Config-rtr-tmplt-af)# route-map RM4-IN in
(R1) (Config-rtr-tmplt-af)# route-map RM4-OUT out
(R1) (Config-rtr-tmplt-af)# exit
(R1) (Config-rtr-tmplt)# address-family ipv6
```

```
(R1) (Config-rtr-tmplt-af)# send-community
(R1) (Config-rtr-tmplt-af)# route-map RM6-IN in
(R1) (Config-rtr-tmplt-af)# route-map RM6-OUT out
(R1) (Config-rtr-tmplt-af)# exit
(R1) (Config-rtr-tmplt)# exit
(R1) (Config-router)# neighbor 172.20.1.2 inherit peer AGGR
(R1) (Config-router)# neighbor 172.20.2.2 inherit peer AGGR
(R1) (Config-router)# address-family ipv6
(R1) (Config-router)# neighbor 172.20.1.2 activate
(R1) (Config-router)# neighbor 172.20.2.2 activate
```

no address-family

To delete all policy commands for an address family in a peer template, use the **no address-family** command.

Format	`no address-family {ipv4 | ipv6}`
Mode	Peer Template Config

Parameter	Description
ipv4	Delete policy parameters for IPv4 routes.
ipv6	Delete policy parameters for IPv6 routes.

activate

Use this command to enable IPv6 unicast exchange in a peer template.

Format	`activate`
Mode	Address Family IPv6

connect-retry-interval

Use this command in Peer Template Configuration mode to add it to a peer template to configure a connection retry interval. If a neighbor does not respond to an initial TCP connection attempt, NETGEAR Managed Switch retries three times. The first retry is after the retry interval configured with the command *neighbor connect-retry-interval* on page 860. Each subsequent retry doubles the previous retry interval. So by default, the TCP connection is retried after 2, 4, and 8 seconds.

If none of the retries is successful, the adjacency is reset to the IDLE state and the IDLE hold timer is started. BGP skips the retries and transitions to IDLE state if TCP returns an error, such as destination unreachable, on a connection attempt.

Default	2 seconds
Format	`connect-retry-interval` *`retry-time`*
Mode	Peer Template Config

Parameter	Description
retry-time	The number of seconds to wait before attempting to establish a TCP connection with a neighbor after a previous attempt failed.

no connect-retry-interval

This command resets to the default the connection retry time in a peer template.

Format	`no connect-retry-interval`
Mode	Peer Template Config

description (Peer Template Config)

Use this command in Peer Template Configuration mode to add to a peer template a text description of a neighbor. The description is informational and has no functional impact.

Default	No description is originated by default.
Format	`description` *`text`*
Mode	Peer Template Config

Parameter	Description
text	Text description of neighbor. Up to 80 characters are allowed.

no description

Use this command to delete the text description of a neighbor from a peer template.

Format	`no description`
Mode	BGP Router Config Peer Template Config

password (Peer Template Config)

Use this command in Peer Template Configuration mode to configure a TCP password in a peer template.

Default	MD5 authentication is disabled.
Format	`password` *`string`*
Mode	Peer Template Config

Parameter	Description
string	Case-sensitive password from 1 to 25 characters in length.

no password

This command disables a TCP password in a peer template.

Format	`no password`
Mode	Peer Template Config

shutdown (Peer Template Config)

Use this command in Peer Template Configuration mode to configure the administration status in a peer template.

Default	Neighbors are not shutdown by default.
Format	`shutdown`
Mode	Peer Template Config

no shutdown

This command administratively enables a BGP peer template.

Format	`no shutdown`
Mode	• BGP Router Config • Peer Template Config

timers

Use this command in Peer Template Configuration mode to configure the keepalive and hold timers in a peer template.

Default	The keepalive and hold timers default to the globally configured values set with the *address-family* command.
Format	`timers` *`keepalive holdtime`*
Mode	Peer Template Config

Parameter	Description
keepalive	The time, in seconds, between BGP KEEPALIVE packets sent to a neighbor. The range is 0 to 65,535 seconds. Jitter is applied to the keepalive interval.
holdtime	The time, in seconds, that BGP continues to consider a neighbor to be alive without receiving a BGP KEEPALIVE or UPDATE packet from the neighbor. If no KEEPALIVE is received from a neighbor for longer than the hold time, BGP drops the adjacency. If the hold time is set to 0, then BGP does not enforce a hold time and BGP does not send periodic KEEPALIVE messages. The range is 0 to 65,535 seconds.

no timers

This command reverts the keep alive and hold time for a peer template to their defaults. After executing this command, the BGP peer must be reset before the changes will take effect.

Format	`no timers`
Mode	Peer Template Config

update-source

Use this command in Peer Template Configuration mode to configure a peer template to use a specific interface as the source for the TCP connection with a neighbor. You can enter an interface in the *`unit/slot/port`* format or a loopback interface in the **`loopback`** *`number`* format.

Default	When no update source is configured, TCP connections use the primary IPv4 address on the outgoing interface to the neighbor.
Format	`update-source [`*`unit/slot/port`*` | loopback `*`number`*`]`
Mode	Peer Template Config

no update-source

This command configures the peer template to use the primary IPv4 address on the outgoing interface to the neighbor for the TCP connection.

Format	`no update-source [`*`unit/slot/port`* `| loopback` *`number`*`]`
Mode	Peer Template Config

timers bgp

This command configures the keepalive and hold times that BGP uses for all of its neighbors.

When BGP establishes an adjacency, the neighbors agree to use the minimum hold time configured on either neighbor. BGP sends KEEPALIVE messages at either 1/3 of the negotiated hold time or the configured keepalive interval, whichever is more frequent.

The new values are not applied to adjacencies already in the ESTABLISHED state. A new keepalive or hold time is applied the next time an adjacency is formed.

Default	The default keepalive time is 30 seconds. The default hold time is 90 seconds.
Format	`timers bgp` *`keepalive holdtime`*
Mode	BGP Router Config

Parameter	Description
keepalive	The time, in seconds, between BGP KEEPALIVE packets sent to a neighbor. The range is 0 to 65,535 seconds. Jitter is applied to the keepalive time.
holdtime	The time, in seconds, that BGP continues to consider a neighbor to be alive without receiving a BGP KEEPALIVE or UPDATE packet from the neighbor. If no KEEPALIVE is received from a neighbor for longer than the hold time, BGP drops the adjacency. If the hold time is set to 0, then BGP does not enforce a hold time and BGP does not send periodic KEEPALIVE messages. The range is 0 to 65,535 seconds.

no timers bgp

This command sets to the default the keepalive and hold times that BGP uses for all of its neighbors.

Format	`no timers bgp`
Mode	BGP Router Config

clear ip bgp

This command resets peering sessions with all or a subnet of BGP peers. The command arguments specify which peering sessions are reset and the type of reset performed. Soft inbound reset causes BGP to send a Route Refresh request to each neighbor being reset. If

a neighbor does not support the Route Refresh capability, then updated policy is applied to routes previously received from the neighbor.

When a change is made to an outbound policy, BGP schedules an outbound soft reset to update neighbors according to the new policy. Use the **interface** option and associated variables to specify if the changes apply to a specific port or to a VLAN.

This command applies to routes for all address families.

Format	`clear ip bgp {* | as-number | neighbor-address} [soft [in | out]][interface [unit/slot/port | vlan-id]]`
Mode	Privileged EXEC

Parameter	Description
*	Reset adjacency with every BGP peer
as-number	Only reset adjacencies with BGP peers in the given autonomous system
neighbor-address	Only reset the adjacency with a single specified peer
soft	(Optional) By default, adjacencies are torn down and reestablished. If the **soft** keyword is given, BGP resends all updates to the neighbors and reprocesses updates from the neighbors.
in or out	(Optional) If the **in** keyword is given, then updates from the neighbor are reprocessed. If the **out** keyword is given, then updates are resent to the neighbor. If neither keyword is given, then updates are reprocessed in both directions.
interface	(Optional) Specifies the interface to clear.
unit/slot/port or vlan-id	(Optional) For *unit/slot/port*, resets only the specified port. For VLAN, resets only the specified *vland-id*.

clear ip bgp counters

This command resets all BGP counters to 0. These counters include send and receive packet and prefix counters for all neighbors.

Format	`clear ip bgp counters`
Mode	Privileged EXEC

debug ip bgp (BGP commands)

To enable debug tracing of BGP events, use the **debug ip bgp** command in privileged EXEC mode. Debug messages are sent to the system log at the DEBUG severity level. To print them on the console, enable console logging at the DEBUG level with the **logging console debug** command (see *logging console* on page 210).

The debug options enabled for a specific peer are the union of the options enabled globally and the options enabled specifically for the peer.

Enabling one of the packet type options enables packet tracing in both the inbound and outbound directions.

Note: To display the debug trace, enable the *debug console* command.

Default	No debug tracing is enabled by default
Format	`debug ip bgp [peer-address | events | keepalives | notification | open | refresh | updates]`
Mode	Privileged EXEC

Parameter	Description
peer-address	(Optional) The IPv4 or IPv6 address of a BGP peer. Debug traces are enabled for a specific peer when this option is specified. The command can be issued multiple times to enable simultaneous tracing for multiple peers.
events	(Optional) Trace adjacency state events.
keepalives	(Optional) Trace transmit and receive of KEEPALIVE packets.
notification	(Optional) Trace transmit and receive of NOTIFICATION packets.
open	(Optional) Trace transmit and receive of OPEN packets.
refresh	(Optional) Traces transmit and receive of ROUTE REFRESH packets.
updates	(Optional) Traces transmit and receive of UPDATE packets.

show ip bgp

To view routes in the BGP routing table, use the **`show ip bgp`** command in Privileged EXEC mode. The output lists both best and nonbest paths to each destination.

Format	`show ip bgp [network/pfx-len [longer-prefixes | shorter-prefixes [length]] | filter-list as-path-list | prefix-list pfx-list-name]`
Mode	Privileged EXEC

Parameter	Description
network/pfx-len	(Optional) Display a specific route identified by its destination prefix
longer-prefixes	(Optional) Used with the network/pfx-len option to show routes whose prefix length is equal to or longer than pfx-len. This option may not be given if the **`shorter-prefixes`** option is given.
shorter-prefixes and length	(Optional) Used with the *`network/pfx-len`* option to show routes whose prefix length is shorter than *`pfx-len`*, and, optionally, longer than a specified length. This option may not be given if the **`longer-prefixes`** option is given.
filter-list as-path-list	(Optional) Filter the output to the set of routes that match a given AS Path list. This option may not be given if a *`network/pfx-len`* option is given, or when a prefix list is given.
pfx-list-name	(Optional) Filter the output to the set of routes that match a given prefix list. This option may not be given if a *`network/pfx-len`* option is given or when a filter list is given.

The command output displays the following information.

Parameter	Description
BGP table version	Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented
Status codes	• s. The route is aggregated into an aggregate address configured with the summary-only option • *. BGP never displays invalid routes; so this code is always displayed • >. Indicates that BGP has selected this path as the best path to the destination • i. If the route is learned from an internal peer
Network	Destination prefix
Next Hop	The route's BGP NEXT HOP
Metric	Multi Exit Discriminator
LocPrf	The local preference
Path	The AS path
Note: The value of the ORIGIN attribute follows immediately after the AS PATH.	

Command example:

```
(R1) # show ip bgp

BGP table version is 5, local router ID is 20.1.1.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            Next Hop     Metric   LocPrf   Path
*> 172.20.1.0/24    100.10.1.1         10      100   20 10        i
                    200.10.1.1
*> 172.20.2.0/24    100.10.1.1         10      100   20 10        ?
```

Command example:

If one or more of the three well-known communities in RFC 1997 are attached to a path, the output of the **show ip bgp** command lists them.

```
(R1) # show ip bgp

BGP table version is 5, local router ID is 20.1.1.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            Next Hop     Metric   LocPrf   Path
*> 172.20.1.0/24    100.10.1.1         10      100   20 10        i
   Communities: no-export
*> 24.95.16.0/24    100.10.1.1         10      100   20 10        i
   Communities: no-advertise
```

```
*> 24.14.8.0/24     100.10.1.1         10      100   20 10        i
   Communities: no-export-subconfed
```

If you enter the command with the *network/pfx-len* option and without any additional options, then the output format lists more information about the individual prefix. The best path is always listed first, followed by any nonbest paths. The output only shows attributes that are included with each path.

Parameter	Description
Prefix/Prefix Length	The destination prefix and prefix length.
Generation ID	The version of the BGP routing table when this route last changed.
Forwarding	Whether this BGP route is used for forwarding.
Advertised To Update Groups	The outbound update groups that this route is advertised to.
Local Preference	The local preference, either as received from the peer or as set according to local policy.
AS Path	The AS Path. This form of show ip bgp displays AS Paths as long as allowed by bgp maxas-limit.
Origin	Value of the ORIGIN attribute.
Metric	Value of the MED attribute, if included.
Type	Whether the path is received from an internal or external peer.
IGP Cost	The interior gateway cost (e.g., OSPF cost) to the BGP NEXT HOP.
Peer (Peer ID)	The IP address of the peer that sent this route, and its router ID.
BGP Next Hop	The BGP NEXT HOP attribute.
Atomic Aggregate	If the ATOMIC AGGEGATE attribute is attached to the path.
Aggregator	The AS number and router ID of the speaker that aggregated the route.
Communities	The BGP communities attached to the path.
Originator	If the ORIGINATOR attribute is attached to the path, the value of this attribute
Cluster List	If the CLUSTER_LIST attribute is attached to the path, the sequence of cluster IDs in the cluster list.

Command example:

```
(R1)  # show ip bgp 172.20.1.0/24

Prefix/Prefix Length..................... 172.20.1.0/24
Generation ID............................ 2056
Forwarding............................... Yes
Advertised to Update Groups.............. 1, 5

Best Path:
Local Preference......................... 100
```

```
AS Path..................................... 20 10
Origin...................................... IGP
Metric...................................... 10
Type........................................ External
IGP Cost.................................... 30
Peer (Peer ID).............................. 100.10.1.1 (32.4.1.1)
BGP Next Hop................................ 100.10.1.1
Atomic Aggregate............................ Included
Aggregator (AS, Router ID).................. 300, 14.1.1.1
Communities................................. no-export

Non-best Paths:
Local Preference............................ 200
AS Path..................................... 18 50 27
Origin...................................... Incomplete
Type........................................ External
IGP Cost.................................... 10
Peer (Peer ID).............................. 200.1.1.1 (18.24.1.3)
BGP Next Hop................................ 200.1.1.1
```

show ip bgp aggregate-address

This command lists aggregate addresses that have been configured and indicates whether each is currently active.

Format	`show ip bgp aggregate-address`
Mode	Privileged EXEC

Parameter	Description
Prefix/Len	Destination prefix and prefix length
AS Set	Indicates whether an empty AS path is advertised with the aggregate address (N) or an AS SET is advertised with the set of AS numbers for the paths contributing to the aggregate (Y)
Summary Only	Indicates whether the individual networks are suppressed (Y) or advertised (N).
Active	Indicates whether the aggregate is currently being advertised.

Command example:

```
(R1) # show ip bgp aggregate-address

Prefix/Len    AS Set    Summary Only    Active

10.0.0.0/8         N               Y         Y
20.0.0.0/8         N               Y         N
```

show ip bgp community

This command shows BGP IPv4 routes that belong to a specified set of communities.

Format	`show ip bgp community` *`communities`* `[exact-match]`
Mode	Privileged EXEC

Parameter	Description
communities	A string of zero or more community values, which may be in either format and may contain the well-known community keywords no-advertise and no-export. The output displays routes that belong to every community specified in the command.
exact-match	(Optional) Only displays routes that are members of those and only those communities specified in the command.

show ip bgp community-list

This command displays IPv4 routes that match a community list name. The output format and field descriptions are the same as for *show ip bgp* on page 890.

Format	`show ip bgp community-list` *`name`* `[exact-match]`
Mode	Privileged EXEC

Parameter	Description
name	A standard community list name.
exact-match	(Optional) Display only routes that are an exact match for the set of communities in the matching community list statement.

show ip bgp neighbors

This command shows details about BGP neighbor configuration and status. If the neighbor is configured to inherit configuration parameters from a peer template, the output shows the inherited values.

Note: Policy configuration is moved from this command to the command **`show ip bgp neighbors policy`**.

Format	`show ip bgp neighbors [`*`neighbor-address`*`]`
Mode	Privileged EXEC

Parameter	Description
neighbor-address	[Optional] The IP address of a neighbor. Used to limit the output to show a single neighbor.

The command output displays the following information.

Parameter	Description
Description	Text string assigned using the command *neighbor filter-list (BGP Router Config)* on page 863. This text string only appears if a description is configured.
Remote Address	The neighbor's IP address
Remote AS	The neighbor's autonomous system number
Peer ID	The neighbor's BGP router ID
Peer Admin Status	START or STOP
Peer State	The adjacency state of this neighbor
Local Interface Address	The IPv4 address used as the source IP address in packets sent to this neighbor.
Local Port	TCP port number on the local end of the connection
Remote Port	TCP port number on the remote end of the connection
Connection Retry Interval	How long BGP waits between connection retries
Neighbor Capabilities	Optional capabilities reported by the neighbor, recognized and accepted by this router. Codes listed in the show output are as follows: • MP. Multiprotocol • RF. Route Refresh This version of NETGEAR Managed Switch does not support any multiprotocol AFI/SAFI pairs other than IPv4 unicast. The presence of this capability does not imply otherwise.
IPv4 Unicast Support	Indicates whether IPv4 unicast routes can be exchanged with this peer. Both indicates that IPv4 is active locally and the neighbor indicated support for IPv4 unicast in its OPEN message. Sent indicates that IPv4 unicast is active locally, but the neighbor did not include this AFI/SAFI pair in its OPEN message. IPv4 unicast is always enabled locally and cannot be disabled.
IPv6 Unicast Support	Indicates whether IPv6 unicast routes can be exchanged with this peer. Both and Sent have the same meaning as for IPv4. None indicates that neither the local router nor the peer has IPv6 enabled for this adjacency. Received indicates that the peer advertised the IPv6 unicast capability, but it is not enabled locally. IPv6 unicast is enabled locally using the neighbor activate command in address-family IPv6 configuration mode.
Update Source	The configured value for the source IP address of packets sent to this peer. This field is only included in the output if the update source is configured.
Configured Hold Time	The time, in seconds, that this router proposes to this neighbor as the hold time

Parameter	Description
Configured Keep Alive Time	The configured KEEPALIVE interval for this neighbor.
Negotiated Hold Time	The minimum of the configured hold time and the hold time in the OPEN message received from this neighbor. If the local router does not receive a KEEPALIVE or UPDATE message from this neighbor within this interval of time, the local router drops the adjacency. This field is only shown if the adjacency state is OPEN CONFIRM or greater.
Keep Alive Time	The number of seconds between KEEPALIVE messages sent to this neighbor. This field is only shown if the adjacency state is OPEN CONFIRM or greater.
MD5 Password	The TCP MD5 password, if one is configured, in plain text
Last Error (Sent)	The last error that occurred on the connection to this neighbor
Last SubError	The suberror reported with the last error.
Established Transitions	The number of times the adjacency has transitioned into the Established state
Established Time	How long since the connection last transitioned to or from the Established state
Time Since Last Update	How long since an UPDATE message has been received from this neighbor
Message Table	The number of BGP messages sent to and received from this neighbor
Received UPDATE Queue Size	Received UPDATE messages are queued for processing. This section shows the current length of the neighbor's UPDATE queue in bytes, the high water mark, the limit, and the number of UPDATEs that have been dropped because the queue reached the limit.
The following fields are displayed for IPv4, and if IPv6 is running, for IPv6 as well.	
Prefixes Advertised	A running count of the number of prefixes advertised to or received from this neighbor
Prefixes Withdrawn	A running count of the number of prefixes included in the Withdrawn Routes portion of UPDATE messages, to and from this neighbor
Prefixes Current	The number of prefixes currently advertised to or received from this neighbor. For inbound prefixes, this count only includes prefixes that passed inbound policy.
Prefixes Accepted	The number of prefixes from this neighbor that are eligible to become active in the local RIB. Received prefixes are ineligible if their BGP Next Hop is not resolvable or if the AS Path contains a loop. A prefix is only considered accepted if it passes inbound policy.
Prefixes Rejected	The number of prefixes currently received from this neighbor that fail inbound policy.
Max NLRI per Update	The maximum number of prefixes included in a single UPDATE message, to and from this neighbor
Min NLRI per Update	The minimum number of prefixes included in a single UPDATE message, to and from this neighbor

Command example:

```
(R1) # show ip bgp neighbors 172.20.1.100
Description: spine 1 router 1

Remote Address ............................... 172.20.1.100
Remote AS .................................... 100
Peer ID ...................................... 14.3.0.1
Peer Admin Status ............................ START
Peer State ................................... ESTABLISHED
Local Interface Address ...................... 172.20.1.2
Local Port ................................... 179
Remote Port .................................. 58265
Connection Retry Interval ..................... 120 sec
Neighbor Capabilities ......................... None
IPv4 Unicast Support .......................... Both
IPv6 Unicast Support .......................... Sent

Update Source.................................
Configured Hold Time .......................... 90 sec
Configured Keep Alive Time..................... 30 sec
Negotiated Hold Time .......................... 30 sec
Keep Alive Time ............................... 10 sec

MD5 Password.................................. password

Last Error (Sent)............................... Hold Timer Expired
Last SubError................................. None
Time Since Last Error.......................... 0 day 0 hr 4 min 27 sec
Established Transitions ....................... 1
Established Time .............................. 0 day 0 hr 4 min 25 sec
Time Elapsed Since Last Update ....................... 0 day 0 hr 4 min 245 sec
Outbound Update Group.......................... 3


             Open   Update   Keepalive   Notification   Refresh   Total
Msgs Sent       1        0          10              0         0      11
Msgs Rcvd       1        1          11              0         0      12

Received UPDATE Queue Size:  0 bytes. High: 355. Limit 196096. Drops 0.

IPv4 Prefix Statistics:
                          Inbound       Outbound
Prefixes Advertised             1              0
Prefixes Withdrawn              0              0
Prefixes Current                1              0
Prefixes Accepted               1            N/A
```

```
Prefixes Rejected                1            N/A
Max NLRI per Update              1              0
Min NLRI per Update              1              0

IPv6 Prefix Statistics:
                           Inbound       Outbound
Prefixes Advertised              1              0
Prefixes Withdrawn               0              0
Prefixes Current                 1              0
Prefixes Accepted                1            N/A
Prefixes Rejected                1            N/A
Max NLRI per Update              1              0
Min NLRI per Update              1              0
```

If the router receives an UPDATE message with an invalid path attribute, the router will in most cases send a NOTIFICATION message and reset the adjacency. BGP maintains a per-neighbor counter for each type of path attribute error. This show command lists each non-zero counter, just after the LastSubError. The counters that may be listed are as follows.

Parameter	Description
Path with duplicate attribute	The peer sent an UPDATE message containing the same path attribute more than once.
Path with well-known/optional conflict	A received path attribute was flagged as both well-known and optional or neither well-known nor optional.
Transitive flag not set on transitive attr	A received path attribute is known to be transitive, but the transitive flag is not set.
Mandatory attribute non-transitive or partial	A mandatory path attribute was received with either the transitive or partial flag set.
Optional attribute non-transitive and partial	An optional path attribute has the transitive flag clear and the partial flag set.
Path attribute too long	A received path attribute was longer than the expected length.
Path attribute length error	A received path attribute has a length value that exceeds the remaining length of the path attributes field.
Invalid ORIGIN code	A received UPDATE message included an invalid ORIGIN code.
Unexpected first ASN in AS path	The AS Path attribute from an external peer did not include the peer’s AS number as the first AS.
Invalid AS path segment type	The AS Path includes a segment with an invalid segment type.

Parameter	Description
Invalid BGP NEXT HOP	The BGP NEXT HOP is not a valid unicast address.
Bad BGP NEXT HOP	The BGP NEXT HOP was either the receiver's IP address or an IP address outside the subnet to the peer.
Invalid AGGREGATOR attribute	The AGGREGATOR attribute was invalid.
Unrecognized well-known path attribute	An UPDATE message contained a path attribute with the Optional flag clear, but this router does not recognize the attribute.
Missing mandatory path attribute	An UPDATE message was received without a mandatory path attribute.
Missing LOCAL PREF attribute	An UPDATE message was received from an internal peer without the LOCAL PREF attribute.
Invalid prefix in UPDATE NLRI	An UPDATE message received from this peer contained a syntactically incorrect prefix.

Command example:

In the following example, BGP has received an UPDATE message from an external peer 172.20.101.100 with something other than the peer's ASN as the first ASN in the AS Path. The additional counter shows that this occurred one time.

```
(NETGEAR Switch) #show ip bgp neighbors 172.20.101.100

Remote Address ............................... 172.20.101.100
Remote AS .................................... 101
...

Last Error ................................... UPDATE Message Error
Last SubError ................................ Malformed AS_PATH
Unexpected first ASN in AS path ............... 1

Established Transitions ...................... 1
Established Time ............................. 0 days 00 hrs 00 mins 10 secs
```

show ip bgp neighbors advertised-routes

This command displays the list of IPv4 routes advertised to a specific neighbor. These are the routes in the adjacent RIB out for the neighbor's outbound update group.

Format	`show ip bgp neighbors` *`ip-address`* `advertised-routes`
Mode	Privileged EXEC

Parameter	Description
ip-address	The IP address of a neighbor.

The command output displays the following information.

Parameter	Description
BGP table version	Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented
Status codes	p – The route has been updated in Adj-RIB-Out since the last UPDATE message was sent. Transmission of an UPDATE message is pending.
Network	Destination prefix
Next Hop	The BGP NEXT HOP as advertised to the peer.
Local Pref	The local preference. Local preference is never advertised to external peers.
Metric	The value of the Multi Exit Discriminator, if the MED is advertised to the peer.
Path	The AS path. The AS path does not include the local AS number, which is added to the beginning of the AS path when a route is advertised to an external peer.
Note: The value of the ORIGIN attribute follows immediately after the AS Path.	

Command example:

```
(NETGEAR Switch) #show ip bgp neighbors 172.20.101.100 advertised-routes

BGP table version is 5, local router ID is 20.1.1.1
Status codes: p advertisement pending
Origin codes: i - IGP, e - EGP, ? - incomplete

Originating default network 0.0.0.0

  Version   Network            Next Hop     Metric   Local Pref  Path
  5         172.20.1.0/24  172.20.101.1         10          100 20 10       i
p 5         20.1.1.0/24    172.20.101.1                     100    20       ?
```

Note: This output differs slightly from the output in **`show ip bgp`** command. Suppressed routes and nonbest routes are not advertised, so these status codes are not relevant here. Advertised routes always have a single next hop, the BGP NEXT HOP advertised to the peer. Local preference is never sent to external peers.

The output indicates whether BGP is configured to originate a default route to this peer (neighbor default-originate).

show ip bgp neighbors policy

This command displays the inbound and outbound IPv4 policies configured for a specific peer. The output distinguishes policies that are configured on the peer itself and policies that the peer inherits from a peer template.

Format	`show ip bgp neighbors [`*`ip-address`*`] policy`
Mode	Privileged EXEC

Parameter	Description
ip-address	Optional. Specifies an IPv4 address of a neighbor to which to limit the output.

The command output displays the following information.

Parameter	Description
Neighbor	The peer address of a neighbor.
Policy	A neighbor-specific BGP policy.
Template	If the policy is inherited from a peer template, this field lists the template name.

Command example:

```
(NETGEAR Switch) #show ip bgp neighbors 172.20.101.100 policy

Neighbor        Policy                           Template
--------------- -------------------------------- ------------------------
172.20.101.100  advertisement-interval 600
 default-originate
 filter-list 500 in
 filter-list 500 out
 prefix-list barney in
 prefix-list wilma out
 maximum-prefix unlimited 100 warning-only      torPeers
 route-map fred in                              torPeers
 route-map dino out                             torPeers
 send-community                                 torPeers
 advertisement-interval 600                     torPeers
 default-originate                              torPeers
```

show ip bgp neighbors received-routes

This command displays the list of routes received from a specific neighbor. The list includes both accepted and rejected routes.

Format	`show ip bgp neighbors` *`ip-address`* `received-routes`
Mode	Privileged EXEC

Parameter	Description
ip-address	The IP address of a neighbor.

The command output displays the following information.

Parameter	Description
Network	Destination prefix
Next Hop	The BGP NEXT HOP as advertised by the peer.
Metric	The value of the Multi Exit Discriminator, if a MED is received from the peer.
Local Pref	The local preference received from the peer.
Path	The AS path as received from the peer
Origin	The value of the Origin attribute as received from the peer

Command example:

```
(NETGEAR Switch) #show ip bgp neighbors 172.20.101.100 received-routes

local router ID is 20.1.1.1
Origin codes: i - IGP, e - EGP, ? - incomplete


Network        Next Hop         Metric   Local Pref  Path  Origin
172.20.1.0/24  172.20.101.1         10          100 20 10       i
20.1.1.0/24    172.20.101.1                     100    20       ?
```

show ip bgp route-reflection

This command displays all global configuration related to IPv4 route reflection, including the cluster ID and whether client-to-client route reflection is enabled, and lists all the neighbors that are configured as route reflector clients.

If a route reflector client is configured with an outbound route map, the output warns that set statements in the route map are ignored when reflecting routes to this client.

Format	`show ip bgp route-reflection`
Mode	Privileged Exec

Parameter	Description
Cluster ID	The cluster ID used by this router. The value configured with the *bgp cluster-id* command is displayed. If no cluster ID is configured, the local router ID is shown and tagged as default.
Client-to-client Reflection	Displays Enabled when this router reflects routes received from its clients to its other clients; otherwise Disabled displays.
Clients	A list of this router's internal peers that have been configured as route reflector clients.
Non-client Internal Peers	A list of this router's internal peers that are not configured as route reflector clients. Routes from non-client peers are reflected to clients and vice-versa.

Command example:

```
(NETGEAR Switch) #show ip bgp route-reflection

Cluster ID ..................................... 1.1.1.1 (configured)
Client-to-client Reflection ................... Enabled
Clients: 172.20.1.2, 172.20.3.2, 172.20.5.2
Non-client Internal Peers: 192.168.1.2, 192.162.2.2
Skipping set statements in outbound route map gandolf when reflecting to internal peer
172.20.1.2.
```

show ip bgp statistics

This command displays recent decision process history. Phase 1 of the decision process reacts to UPDATE messages received from peers, determining what new routes are accepted and deleting withdrawn routes from the Adj-RIB-In. Phase 2 determines the best path for each destination, updates the BGP route table, and updates the common RIB. Phase 3 is run independently for each outbound update group and determines which routes should be advertised to neighbors in each group. Each entry in the table shows statistics for one phase of the decision process. The table shows the 20 most recent decision process runs, with the most recent information at the end of the table.

Format	`show ip bgp statistics`
Mode	Privileged EXEC

The command displays the following information.

Parameter	Description
Delta T	How long since the decision process was run. hours:minutes:seconds if the elapsed time is less than 24 hours. Otherwise, days:hours.
Phase	Which phase of the decision process was run
Upd Grp	Outbound update group ID. Only applies when phase 3 is run.

Parameter	Description
GenId	Generation ID of BGP routing table when decision process was run. The generation ID is incremented each time phase 2 of the decision process is run and when there is a change to the status of aggregate addresses.
Reason	The event that triggered the decision process to run
Peer	Phase 1 of the decision process can be triggered for a specific peer when a peer's inbound routing policy changes or the peer is reset. When phase 1 is run for a single peer, the peer's IP address is given.
Duration	How long the decision process took, in milliseconds
Adds	The number of routes added. For phase 1, this is the number of prefixes that pass inbound policy and are added to the Accept-RIB-In. For phase 2, this is the number of routes added to the BGP routing table. For phase 3, this is the number of prefixes added to the update group's Adj-RIB-Out.
Mods	The number of routes modified. Always 0 for phase 1.
Dels	The number of routes deleted. Always 0 for phase 1.

Command example:

```
(R1) # show ip bgp statistics

  Delta T  Phase  Upd Grp   GenId          Reason       Peer  Duration  Adds  Mods  Dels
 29:33:49      3        0    2041  Fwd status chng                 34   750     0   500
 29:33:40      2             2042   Accept-RIB-In-                 59   750     0   500
 29:33:28      2             2043   Accept-RIB-In-                 10     0     0   250
 29:23:40      2             2044   Accept-RIB-In-                 32     0     0  1000
 29:13:40      3        1    2044     Phase 2 done                 48   500  2500  1750
 29:02:40      1             2044      Adj-RIB-In+    0.0.0.0       21   500     0     0
 29:02:01      3        0    2044     Phase 2 done                 41   750     0  1250
 28:33:40     2            2045    Phase 1 done                   32   500     0
 28:15:00      1             2045      Adj-RIB-In+    0.0.0.0        9   250     0     0
 28:14:40      2            2046     Phase 1 done                     16   250     0
```

show ip bgp summary

This command displays a summary of BGP configuration and status.

Format	`show ip bgp summary`
Mode	Privileged EXEC

The command displays the following information.

Parameter	Description
IPv4 Routing	Displays whether IPv4 routing is globally enabled. BGP does not include the IPv4 unicast AFI/SAFI capability in OPEN messages it sends unless routing is globally enabled.
BGP Admin Mode	Displays whether BGP is globally enabled
BGP Router ID	The configured router ID
Local AS Number	The router's AS number
Traps	Displays whether BGP traps are enabled.
Maximum Paths	The maximum number of next hops in an external BGP route.
Maximum Paths iBGP	The maximum number of next hops in an internal BGP route.
Default Keep Alive Time	The configured keepalive time used by all peers that have not been configured with a peer-specific keepalive time.
Default Hold Time	The configured hold time used by all peers that have not been configured with a peer-specific hold time.
Number of Network Entries	The number of distinct prefixes in the local RIB
Number of AS Paths	The number of AS paths in the local RIB
Default Metric	The default value for the MED for redistributed routes.
Default Route Advertise	Whether BGP is configured to advertise a default route. Corresponds to the *default-information originate (BGP Router Config)* command.
Redistributing Source	A source of routes that BGP is configured to redistribute.
Metric	The metric configured with the redistribute command.
Match Value	For routes redistributed from OSPF, the types of OSPF routes being redistributed.
Distribute List	The name of the prefix list used to filter redistributed routes, if one is configured with the *distribute-list prefix out (BGP)* command.
Route Map	The name of the route map used to filter redistributed routes.
Neighbor	The IP address of a neighbor
ASN	The neighbor's ASN
MsgRcvd	The number of BGP messages received from this neighbor
MsgSent	The number of BGP messages sent to this neighbor
State	The adjacency state. One of IDLE, CONNECT, ACTIVE, OPEN SENT, OPEN CNFRM, EST

Parameter	Description
Up/Down Time	Displays how long the adjacency has been in the ESTABLISHED state, or, if the adjacency is down, how long it has been down. In days:hours:minutes:seconds
Pfx Rcvd	The number of prefixes received from the neighbor

Command example:

```
(R1) # show ip bgp summary

IPv4 Routing.............................Enable
BGP Admin Mode...........................Enable
BGP Router ID............................172.20.1.1
Local AS Number..........................200
Traps....................................Disable
Maximum Paths............................32
Maximum Paths iBGP.......................16
Default Keep Alive Time..................30 sec
Default Hold Time........................90 sec
Number of Network Entries................20
Number of AS Paths.......................5

Default Metric.............................. Not configured
Default Route Advertise...................... No

Redistributing..............................
Source...................................... ospf
Metric...................................... Not Configured
Match Value................................. 'internal'
Distribute List............................. Not configured

Neighbor      ASN    MsgRcvd  MsgSent      State  Up/Down Time   Pfx Rcvd
100.10.1.1     50         48       92        EST      00:47:30         20
100.20.1.4     20          0        2   OPEN SENT                        0
```

show ip bgp template

Use this command to view information about all configured BGP peer templates or for the specified BGP template that you can specify with the *name* variable.

Format	`show ip bgp template [`*name*`]`
Mode	Privileged Exec

Term	Definition
Name	The name of a BGP peer template
AF	The address family to which the configuration command applies. This field is blank for session parameters, which apply to all address families.
Configuration	Configuration commands that are included in the template.

Command example:

```
(NETGEAR Switch) #show ip bgp template

Template Name   AF    Configuration
-------------  ----   ----------------------------
peer-grp1              timers 5 15
                       password rivendell
               IPv4    advertisement-interval 15


peer-grp2      IPv4    prefix-list strider in
               IPv4    maximum-prefix 100
               IPv6    prefix-list gandolf in
               IPv6    maximum-prefix 200

peer-grp3      IPv6    send-community

peer-grp4              update-source loopback 0
               IPv4    next-hop-self
```

show ip bgp traffic

This command reports global BGP message counters for transmitted and received messages along with BGP work queue information.

Format	`show ip bgp traffic`
Mode	Privileged Exec

The first table lists the number of BGP messages of each type that this router has sent and received. Following the table is a maximum send and receive UPDATE message rate. These rates report the busiest one-second interval.

The queue statistics table reports information for BGP work queues. Items placed on each of these work queues are as follows:

Term	Description
Events	Includes most timer events and configuration changes.
Keepalive Tx	Includes timer events to send a KEEPALIVE message to a peer.
Dec Proc	Includes events that cause the decision process to be run.
Rx Data	holds incoming BGP messages.
RTO Notifications	Includes best route change and next hop resolution change notifications from the routing table.
MIB Queries	Includes pending SNMP queries for BGP status

Command example:

```
(NETGEAR Switch) #show ip bgp traffic

Time Since Counters Cleared: 55223 Seconds
BGP Message Statistics
                Open     Update  Notification    Keepalive    Refresh      Total
Recd:              6         11             0         7888          0       7905
Sent:              8         56             3         8465          0       8532

Max Received UPDATE rate: 1 pps
Max Send UPDATE rate: 5 pps

BGP Queue Statistics
             Current         Max       Drops       Limit
Events             0           2           0         800
Keepalive Tx       0           3           0         128
Dec Proc           0           3           0         133
Rx Data            0           3           0         500
RTO Notifications  0           4           0        1222
MIB Queries        0           0           0           5
```

show ip bgp update-group

This command reports the status of outbound update groups and their members.

Format	`show ip bgp update-group [`*`group-index`* `|` *`peer-address`*`]`
Mode	Privileged EXEC

Parameter	Description
group-index	(Optional) If specified, this option restricts the output to a single update group.
peer-address	(Optional) If specified, this option restricts the output to the update group containing the peer with the given address.

The command displays the following information.

Parameter	Description
Update Group ID	Unique identifier for outbound update group
Peer Type	Whether peers in this update group are internal or external
Minimum Advertisement Interval	The minimum time, in seconds, between sets of UPDATE messages sent to the group
Send Community	If BGP communities are included in route advertisements to members of the group.
Remove Private ASNs	If BGP removes private ASNs from paths advertised to members of this update group. • Replace if BGP replaces private ASNs with the local ASN. • Remove if private ASNs are removed. • Otherwise No.
Route Reflector Client	If peers in this update group are route reflector clients.
Neighbor AS Path Access List Out	The AS path access list used to filter UPDATE messages sent to peers in the update group
Neighbor Prefix List Out	Name of the prefix list used to filter prefixes advertised to the peers in the update group
Members Added	The number of peers added to the group since the group was formed
Members Removed	The number of peers removed from the group
Update Version	The number of times phase 3 of the BGP decision process has run for this group to determine which routes should be advertised to the group
Number of UPDATEs Sent	The number of UPDATE messages that have been sent to this group. Incremented once for each UPDATE regardless of the number of group members
Time Since Last UPDATE	Time since an UPDATE message was last sent to the group. If no UPDATE has been sent to the group, the status is Never.
Current Prefixes	The number of prefixes currently advertised to the group
Current Paths	The number of paths currently advertised to the group
Prefixes Advertised	The total number of prefixes advertised to the group since the group was formed
Prefixes Withdrawn	The total number of prefixes included in the Withdrawn Routes field of UPDATE messages sent to the group since the group was formed

Parameter	Description
UPDATE Send Failures	The number of UPDATE messages that failed to be delivered to all members of the group
Current Members	The IPv4 address of all current members of the group

The update send history table show statistics on as many as the ten most recent executions of the update send process for the update group. Items in the history table are as follows.

Parameter	Description
Version	The update version
Delta T	The amount of time elapsed since the update send process executed. hours::minutes::seconds.
Duration	How long the update send process took, in milliseconds.
UPD Built	The number of UPDATE messages built
UPD Sent	The number of UPDATE messages successfully transmitted to group members. Normally a copy of each UPDATE message built is sent to each group member.
Paths Sent	The number of paths advertised.
Pfxs Adv	The number of prefixes advertised
Pfxs Wd	The number of prefixes withdrawn

Command example:

The following example displays information for all update groups:

```
(R1) # show ip bgp update-group

Update Group ID.............................. 0
Peer Type.................................... External
Minimum Advertisement Interval.............. 30 seconds
Send Community............................... Yes
Remove Private ASNs.......................... No
Route Reflector Client....................... No
Neighbor AS Path Access List Out............ 1
Neighbor Prefix List Out..................... pfxList1
Members Added................................ 48
Members Removed.............................. 0
Update Version............................... 19
Number of UPDATEs Sent....................... 512
Time Since Last Update....................... 5 hrs 3 min 2 sec
Current Prefixes............................. 5500
Current Paths................................ 22
Prefixes Advertised.......................... 191250
Prefixes Withdrawn........................... 186000
UPDATE Send Failures......................... 0
```

```
Current Members:  172.20.1.100, 172.20.2.100

   Version   Delta T Duration UPD Built UPD Sent Paths Sent Pfxs Adv  Pfxs Wd
        10   00:33:49      100         6      288          5     1250      750
        11   00:33:49        0         4      192          3      750      250
        12   00:33:49        0         2       96          1      250     1000
        13   00:33:49        0         2       96          1      250     1018
        14   00:33:49        0         1       48          0        0      482
        15   00:33:49      100         8      384          7     1750      750
        16   00:33:49        0         3      144          2      500      250
        17   00:31:49        0         4      192          3      750      750
        18   00:23:49      100         4      192          3      750     1000
        19   00:03:49      100         6      288          5     1250      500


Update Group ID.......................... 1
Peer Type................................ Internal
Minimum Advertisement Interval........... 5 seconds
Remove Private ASNs...................... No
Route Reflector Client................... No
Send Community........................... Yes
Neighbor AS Path Access List Out......... none
Neighbor Prefix List Out................. none
Members Added............................ 3
Members Removed.......................... 0
Update Version........................... 4
Number of UPDATEs Sent................... 8
Time Since Last UPDATE................... 3 hrs 13 min 22 sec
Current Prefixes......................... 84
Current Paths............................ 2
Prefixes Advertised...................... 100
Prefixes Withdrawn....................... 16
UPDATE Send Failures..................... 0

Current Members:  172.24.3.1, 172.25.8.56, 172.28.9.1

Version   Delta T Duration UPD Built UPD Sent Paths Sent Pfxs Adv  Pfxs Wd
     10   00:00:49      100         6      288          5     1250      750
```

show bgp ipv6

Use the **show bgp ipv6** command in Privileged EXEC mode to display IPv6 routes in the BGP routing table.

Format	show bgp ipv6 [*ipv6-prefix/prefix-length* [longer-prefixes | shorter-prefixes [*length*]] | filter-list *as-path-list*]
Mode	Privileged Exec

Parameter	Description
ipv6-prefix/ prefix-length	(Optional) Limits the output to a specific prefix.
longer-prefixes	(Optional) Display the specified prefix and any longer prefixes within the same range.
shorter-prefixes	(Optional) Used with the *ipv6-prefix/prefix-length* option to show routes whose prefix length is shorter than *prefix-length* and, optionally, longer than a specified length. This option may not be given if the **longer-prefixes** option is given.
as-path-list	(Optional) Filter the output to the set of routes that match a given AS Path list. This option may not be given if an *ipv6-prefix/prefix-length* option is given.

The command output displays the following information.

Parameter	Description
BGP table version	Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented
Status codes	• s. The route is aggregated into an aggregate address configured with the summary-only option • *. BGP never displays invalid routes; so this code is always displayed • >. Indicates that BGP has selected this path as the best path to the destination • i. If the route is learned from an internal peer
Network	IPv6 destination prefix
Next Hop	The IPv6 route's BGP NEXT HOP
Metric	Multi Exit Discriminator
LocPrf	The local preference
Path	The AS path
Origin	The value of the Origin attribute

Command example:

```
(R1) # show bgp ipv6

BGP table version is 5, local router ID is 20.1.1.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
   Network               Next Hop     Metric   LocPrf   Path
*> 2001:DB8::/48       3FFE:100::1        10      100   20 10  i
                       3FFE:200::4
*> 2001:DB8:4:5::/64   3FFE:100::1        10      100   20 10  ?
```

show bgp ipv6 aggregate-address

This command lists IPv6 aggregate addresses that have been configured and indicates whether each is currently active.

Format	`show bgp ipv6 aggregate-address`
Mode	Privileged Exec

Parameter	Description
Prefix/Len	Destination prefix and prefix length.
AS Set	Indicates whether an empty AS path is advertised with the aggregate address (N) or an AS SET is advertised with the set of AS numbers for the paths contributing to the aggregate (Y).
Summary Only	Indicates whether the individual networks are suppressed (Y) or advertised (N).
Active	Indicates whether the aggregate is currently being advertised.

Command example:

```
(R1) # show bgp ipv6 aggregate-address

Prefix/Len         AS Set    Summary Only    Active
----------------   ------    ------------    ------
2001:DB8::/48           N               Y         Y
3ffe:4000:1::/48        N               Y         Y
```

show bgp ipv6 community

This command displays IPv6 routes that belong to a given set of communities. The output format and field descriptions are the same as for the command *show bgp ipv6* on page 912.

Format	`show bgp ipv6 community` *communities* `[exact-match]`
Mode	Privileged Exec

Parameter	Description
communities	A string of zero or more community values, which may be in either format and may contain the well-known community keywords no-advertise and no-export. The output displays routes that belong to every community specified in the command.
exact-match	(Optional) Only displays routes that are members of those and only those communities specified in the command.

show bgp ipv6 community-list

This command displays IPv6 routes that match a community list. The output format and field descriptions are the same as for the command *show bgp ipv6* on page 912.

Format	`show bgp ipv6 community-list` *`name`* `[exact-match]`
Mode	Privileged Exec

Parameter	Description
name	A standard community list name.
exact-match	(Optional) Display only routes that are an exact match for the set of communities in the matching community list statement.

show bgp ipv6 neighbors advertised-routes

This command displays IPv6 routes advertised to a specific neighbor. The format and field descriptions are the same as for the IPv4 command *show ip bgp neighbors advertised-routes* on page 899, except that the Network and Next Hop fields show IPv6 addresses.

Format	`show bgp ipv6 neighbors {`*`ipv4-address`* `|` *`ipv6-address`*`} advertised-routes`
Mode	Privileged Exec

show bgp ipv6 neighbors

This command displays a list of IPv6 routes received from a specific neighbor. The list includes either all routes received from the neighbor, received routes that passed inbound policy, or routes rejected by inbound policy. The output and format as the same as for the IPv4 command *show ip bgp neighbors* on page 894, except that they list IPv6 routes.

Format	`show bgp ipv6 neighbors {`*`ipv4-address`* `|` *`ipv6-address`*`} {received-routes | routes | rejected-routes}`
Mode	Privileged Exec

show bgp ipv6 neighbors policy

Use this command displays the inbound and outbound IPv6 policies configured for a specific peer. The output distinguishes policies that are configured on the peer itself and policies that the peer inherits from a peer template. Specifying an IPv4 or IPv6 address limits the output to a single neighbor. If the neighbor's address is a link local address, the interface must be specified.

Format	`show bgp ipv6 neighbors [`*`ipv4-address`*` | `*`ipv6-address`*` [interface `*`interface-name`*`]] policy`
Mode	Privileged Exec

show bgp ipv6 route-reflection

This command shows the configuration of the local router as a route reflector.

Format	`show bgp ipv6 route-reflection`
Mode	Privileged Exec

Parameter	Description
Cluster ID	The cluster ID used by this router. The value configured with the *bgp cluster-id* command is displayed. If no cluster ID is configured, the local router ID is shown and tagged as default.
Client-to-client Reflection	Displays *Enabled* when this router reflects routes received from its clients to its other clients; otherwise *Disabled* displays.
Clients	A list of this router's internal peers that have been configured as route reflector clients.
Non-client Internal Peers	A list of this router's internal peers that are not configured as route reflector clients. Routes from non-client peers are reflected to clients and vice-versa.

Command example:

```
(NETGEAR Switch) #show bgp ipv6 route-reflection

Cluster ID ..................................... 0.0.0.0 (default)
Client-to-client Reflection .................... Enabled
Clients:
Non-client Internal Peers:
```

show bgp ipv6 statistics

This command shows statistics for the IPv6 decision process. Output and field descriptions are the same as for the IPv4 command *show ip bgp statistics* on page 903.

Format	`show bgp ipv6 statistics`
Mode	Privileged Exec

show bgp ipv6 summary

This command displays a summary of BGP IPv6 configuration and status. The output and field descriptions are the same as for the command *show ip bgp summary* on page 904, except that Number of Network Entries, Number of AS Paths, and Pfx Rcvd all count IPv6 rather than IPv4 routing information. The command lists all adjacencies that are configured to carry IPv6 routes.

Format	`show bgp ipv6 summary`
Mode	Privileged Exec

show bgp ipv6 update-group

This command reports the status of IPv6 outbound update groups and their numbers. Output and format are the same as for *show ip bgp template* on page 906.

Format	`show bgp ipv6 update-group [group-index | peer-address]`
Mode	Privileged Exec

Parameter	Description
group-index	(Optional) If specified, this option restricts the output to a single update group.
peer-address	(Optional) If specified, this option restricts the output to the update group containing the peer with the given address.

Routing Policy Commands

Exterior routing protocols like BGP use industry-standard routing policy to filter and modify routing information exchanged with peers. BGP makes use of the following routing policy constructs:

- AS Path Access Lists
- BGP Community Lists
- Use the Routing Policy commands to configure routing policies such as:
- Matching on an AS Path
- Modifying the AS Path
- Setting the local preference
- Setting the route metric
- Setting an IPv6 next hop
- Setting or matching on a BGP community

ip as-path access-list

To create an AS path access list, use the **ip as-path access-list** command in Global Configuration mode. An AS path access list filters BGP routes on the AS path attribute of a BGP route. The AS path attribute is a list of the autonomous system numbers along the path to the destination. An AS path access list is an ordered sequence of statements. Each statement specifies a regular expression and a permit or deny action. If the regular expression matches the AS path of the route expressed as an ASCII string, the route is considered a match and the statement's action is taken. An AS path list has an implicit deny statement at the end. If a path does not match any of the statements in an AS path list, the action is considered to be deny.

Once you have created an AS path list, you cannot delete an individual statement. If you want to remove an individual statement, you must delete the AS path list and recreate it without the statement to be deleted.

Statements are applied in the order in which they are created. New statements are added to the end of the list. The statement with the first matching regular expression is applied.

NETGEAR Managed Switch allows configuration of up to 128 AS path access lists, with up to 64 statements each.

To enter the question mark within a regular expression, you must first enter **Ctrl-V** to prevent the CLI from interpreting the question mark as a request for help.

Table 13 on page 917 lists AS path list regular expression syntax.

Default	No AS path lists are configured by default. There are no default values for any of the parameters of this command.
Format	`ip as-path access-list` *`as-path-list-number`* `{permit | deny}` *`regexp`*
Mode	Global Configuration

Parameter	Description
as-path-list-number	A number from 1 to 500 uniquely identifying the list. All AS path access list commands with the same as-path-list-number are considered part of the same list.
permit	(Optional) Permit routes whose AS Path attribute matches the regular expression.
deny	(Optional) Deny routes whose AS Path attribute matches the regular expression.
regexp	A regular expression used to match the AS path attribute of a BGP path where the AS path is treated as an ASCII string.

Table 13. AS path regular expression syntax

Special Character	Symbol	Behavior
asterisk	*	Matches zero or more sequences of the pattern.
brackets	[]	Designates a range of single-character patterns.
caret	^	Matches the beginning of the input string.

Table 13. AS path regular expression syntax

Special Character	Symbol	Behavior
dollar sign	$	Matches the end of the input string.
hyphen	–	Separates the end points of a range.
period	.	Matches any single character, including white space.
plus sign	+	Matches 1 or more sequences of the pattern.
question mark	?	Matches 0 or 1 occurrences of the pattern.
underscore	_	Matches a comma (,), left brace ({), right brace (}), left parenthesis, right parenthesis, the beginning of the input string, the end of the input string, or a space.

Command example:

The following example configures the router to reject routes that it receives from neighbor 172.20.1.1 with an AS path that indicates that the route originates in, or passes through, AS 100:

```
(NETGEAR Switch)(Config)# ip as-path access-list 1 deny _100_
(NETGEAR Switch)(Config)# ip as-path access-list 1 deny ^100$
(NETGEAR Switch)(Config)# router bgp 1
(NETGEAR Switch)(Config-router)# neighbor 172.20.1.1 remote-as 200
(NETGEAR Switch)(Config-router)# neighbor 172.20.1.1 filter-list 1 in
```

no ip as-path access-list

To delete an AS path access list, use the **`no ip as-path access-list`** command.

Format	`no ip as-path access-list` *`as-path-list-number`*
Mode	Global Configuration

ip bgp-community new-format

To display BGP standard communities in AA:NN format, use the **`ip bgp-community new-format`** command in Global Configuration mode. RFC 1997 specifies that the first two bytes of a community number are considered to be an autonomous system number. The new format displays a community number as the ASN followed by a 16-bit AS-specific number.

Default	Standard communities are displayed in AA:NN format.
Format	`ip bgp-community new-format`
Mode	Global Configuration

no ip bgp-community new-format

To display BGP standard communities as 32-bit integers, use the **no ip bgp-community new-format** command.

Format	no ip bgp-community new-format
Mode	Global Configuration

ip community-list

To create or configure a BGP community list, use the **ip community-list** command in Global Configuration mode. A community list statement with no community values is considered a match for all routes, regardless of their community membership. So the statement **ip community-list bullseye permit** is a *permit all* statement.

A community number may be entered in either format, as a 32-bit integer or a pair of 16-bit integers separated by a colon, regardless of whether the *ip bgp-community new-format* command is active. Up to 16 communities, including the well-known communities, can be listed in a single command. Up to 32 statements may be configured with a given community list name. Up to 128 unique community list names may be configured.

Default	No community lists are configured by default.
Format	ip community-list standard *list-name* {permit | deny} [*community-number*] [no-advertise] [no-export]
Mode	Global Configuration

Parameter	Description
standard list-name	Identifies a named standard community list. The name may contain up to 32 characters.
permit	Indicates that matching routes are permitted.
deny	Indicates that matching routes are denied.
community-number	From zero to 16 community numbers formatted as a 32-bit integers or in AA:NN format, where AA is a 2-byte autonomous system number and NN is a 16 bit integer. The range is 1 to 4,294,967,295 (any 32-bit integer other than 0). Communities are separated by spaces.
no-advertise	The well-known standard community, NO_ADVERTISE (0xFFFFFF02).
no-export	The well-known standard community, NO_EXPORT, (0xFFFFFF01).

no ip community-list

To delete a community list, use the **no ip community-list** command.

Format	no ip community-list standard *list-name*
Mode	Global Configuration

show ip as-path-access-list

This command displays the contents of AS path access lists.

Format	`show ip as-path-access-list [as-path-list-number]`
Mode	Privileged EXEC

Parameter	Description
as-path-list-number	(Optional) When an AS path list number is specified, the output is limited to the single AS path list specified. The number is an integer from 1 to 500.

Command example:

```
(NETGEAR Switch)# show ip as-path-access-list

AS path access list 1
deny _100_
deny ^100$

AS path access list 2
deny _200_
deny ^200$
```

show ip community-list

This command displays community lists. The format of community values is dictated by the command *ip bgp-community new-format* on page 918.

Format	`show ip community-list [community-list-name]`
Mode	Privileged EXEC

Parameter	Description
community-list-name	(Optional) A standard community list name. This option limits the output to a single list.

Command example:

```
(NETGEAR Switch) #show ip community-list

Standard community list buzz
     permit 100:200
     permit 100:300
     permit 100:400
Standard community list woody
    permit 200:1
    permit 200:2
    permit 200:3
```

clear ip community-list

This command clears community lists.

Format	`clear ip community-list [`*`community-list-name`*`]`
Mode	Privileged EXEC

Parameter	Description
community-list-name	(Optional) A community list name.

IPv6 Commands

13

This chapter describes the IPv6 commands available in the NETGEAR Managed Switch CLI. The chapter contains the following sections:

- *IPv6 Management Commands*
- *Tunnel Interface Commands*
- *Loopback Interface Commands*
- *IPv6 Routing Commands*
- *OSPFv3 Commands*
- *DHCPv6 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.

Only the following switches support IPv6 Management:

- M6100
- M5300-28G3
- M5300-52G3
- M5300-28GF3

The following switches support IPv6 with an L3 license:

- M5300-28G
- M5300-52G
- M5300-28G-POE+
- M5300-52G-POE+

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 NETGEAR Managed Switch software, dual IPv4/IPv6 operation over the service port is enabled. NETGEAR Managed Switch software has capabilities such as:

- 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).

serviceport ipv6 enable

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

Note: This command is supported on M6100 series switches only

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

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.

Note: This command is supported on M6100 series switches only

Format	`serviceport ipv6 address {`*`address/prefix-length`* `[eui64] | autoconfig | dhcp}`
Mode	Privileged EXEC

Parameter	Description
address	IPv6 prefix in IPv6 global address format.
prefix-length	IPv6 prefix length value.
eui64	Formulate IPv6 address in eui64 address format.
autoconfig	Configure stateless global address autoconfiguration capability.
dhcp	Configure dhcpv6 client protocol.

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	`no serviceport ipv6 address {`*`address/prefix-length`* `[eui64] | autoconfig | dhcp}`
Mode	Privileged EXEC

serviceport ipv6 gateway

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

Note: Only a single IPv6 gateway address can be configured for the service port. There may 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 their service port interface.

Note: This command is supported on M6100 series switches only

Format	`serviceport ipv6 gateway` *`gateway-address`*
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	`no serviceport ipv6 gateway`
Mode	Privileged EXEC

serviceport ipv6 neighbor

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.

Note: This command is supported on M6100 series switches only

Format	`serviceport ipv6 neighbor` *`ipv6-address macaddr`*
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	`no serviceport ipv6 neighbor` *`ipv6-address macaddr`*
Mode	Privileged EXEC

show network ipv6 neighbors

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

Default	None
Format	`show network ipv6 neighbors`
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; FALSE it is not a router.
Neighbor State	The state of the neighbor cache entry. 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.
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.

Command example:

```
(NETGEAR Routing) #show network ipv6 neighbors

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

show serviceport ipv6 neighbors

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.

Note: This command is supported on M6100 series switches only

Default	None
Format	`show serviceport ipv6 neighbors`
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 Routing) #show serviceport ipv6 neighbors

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

ping ipv6

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 argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the unit/slot/port format. 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 *vland-id* argument, **serviceport** keyword, or **network** 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	ping ipv6 {*ipv6-global-address* | *hostname* | {interface {*unit/slot/port* | *vlan vland-id* | serviceport | network} *link-local-address*} [size *datagram-size*]}
Mode	Privileged EXEC User Exec

ping ipv6 interface

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, tunnel, vlan, or physical interface as the source.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the *unit/slot/port* format. 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	ping ipv6 interface {*unit/slot/port* | vlan *vland-id* | loopback *loopback-id* | network | serviceport | tunnel *tunnel-id*} {link-local-address *link-local-address* | *ipv6-address*} [size *datagram-size*]
Modes	Privileged EXEC User Exec

Tunnel Interface Commands

The commands in this section describe how to create, delete, and manage tunnel interfaces.Several different types of tunnels provide functionality to facilitate the transition of IPv4 networks to IPv6 networks. These tunnels are divided into two classes: configured and automatic. The distinction is that configured tunnels are explicitly configured with a destination or endpoint of the tunnel. Automatic tunnels, in contrast, infer the endpoint of the tunnel from the destination address of packets routed into the tunnel. To assign an IP address to the tunnel interface, see *ip address* on page 668. To assign an IPv6 address to the tunnel interface, see *ipv6 address* on page 934.

Note: Tunnel interface commands are supported on the M5300 and M6100 series switches only.

interface tunnel

Use this command to enter the Interface Config mode for a tunnel interface. The *tunnel-id* range is 0 to 7.

Format	interface tunnel *tunnel-id*
Mode	Global Config

no interface tunnel

This command removes the tunnel interface and associated configuration parameters for the specified tunnel interface.

Format	`no interface tunnel` *`tunnel-id`*
Mode	Global Config

tunnel source

This command specifies the source transport address of the tunnel, either explicitly or by reference to an interface.

Format	`tunnel source {`*`ipv4-address`* `| ethernet` *`unit/slot/port`*`}`
Mode	Interface Config

tunnel destination

This command specifies the destination transport address of the tunnel.

Format	`tunnel destination` *`ipv4-address`*
Mode	Interface Config

tunnel mode ipv6ip

This command specifies the mode of the tunnel. With the optional 6to4 argument, the tunnel mode is set to 6to4 automatic. Without the optional 6to4 argument, the tunnel mode is configured.

Format	`tunnel mode ipv6ip [6to4]`
Mode	Interface Config

show interface tunnel

This command displays the parameters related to tunnel such as tunnel mode, tunnel source address and tunnel destination address.

Format	`show interface tunnel [`*`tunnel-id`*`]`
Mode	Privileged EXEC

If you do not specify a tunnel ID, the command shows the following information for each configured tunnel.

Term	Definition
Tunnel ID	The tunnel identification number.
Interface	The name of the tunnel interface.
Tunnel Mode	The tunnel mode.
Source Address	The source transport address of the tunnel.
Destination Address	The destination transport address of the tunnel.

If you specify a tunnel ID, the command shows the following information for the tunnel.

Term	Definition
Interface Link Status	Shows whether the link is up or down.
MTU Size	The maximum transmission unit for packets on the interface.
IPv6 Address/Length	If you enable IPv6 on the interface and assign an address, the IPv6 address and prefix display.

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 668. To assign an IPv6 address to the loopback interface, see *ipv6 address* on page 934.

interface loopback

Use this command to enter the Interface Config mode for a loopback interface. The range of the loopback ID is 0 to 7.

Format	`interface loopback` *`loopback-id`*
Mode	Global Config

no interface loopback

This command removes the loopback interface and associated configuration parameters for the specified loopback interface.

Format	`no interface loopback` *`loopback-id`*
Mode	Global Config

show interface loopback

This command displays information about configured loopback interfaces.

Format	`show interface loopback [`*`loopback-id`*`]`
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.

Note: IPv6 routing commands are supported on the M5300 and M6100 series switches only.

ipv6 hop-limit

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	`ipv6 hop-limit` *hops*
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

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

Use this command to enable IPv6 routing on an interface or range of interfaces, including tunnel and loopback interfaces, that has 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

Use this command to configure an IPv6 address on an interface or range of interfaces, including tunnel and loopback interfaces, and to enable IPv6 processing on this interface. 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`* 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`** field designates that IPv6 processing on the interfaces was 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.

Format	`ipv6 address` *`prefix/prefix_length`* `[eui64]`
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`* designates how many of the high-order contiguous bits of the address

comprise the prefix.The optional **eui-64** field designates that IPv6 processing on the interfaces was enabled using an EUI-64 interface ID in the low order 64 bits of the address.

If you do not supply any parameters, the command deletes all the IPv6 addresses on an interface.

Format	`no ipv6 address [prefix/prefix_length] [eui64]`
Mode	Interface Config

ipv6 address autoconfig

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	`ipv6 address autoconfig`
Mode	Interface Config

no ipv6 address autoconfig

This command the IPv6 autoconfiguration status on an interface to the default value.

Format	`no ipv6 address autoconfig`
Mode	Interface Config

ipv6 address dhcp

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	`ipv6 address dhcp`
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

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 the router 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.

You can specify a *unit/slot/port* or *vlan-id* or *tunnel_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 *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the *unit/slot/port* format. 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 *ipv6-prefix/prefix_length* {*next-hop-address* | Null0 | interface {*unit/slot/port* | vlan *vlan-id* | tunnel *tunnel_id*} *next-hop-address*} [*preference*]
Mode	Global Config

no ipv6 route

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	no ipv6 route *ipv6-prefix/prefix_length* [{*next-hop-address* | Null0 | interface {*unit/slot/port*| vlan *vland-id* | tunnel *tunnel_id*} *next-hop-address*} [*preference*]]
Mode	Global Config

ipv6 route distance

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	ipv6 route distance *preference*
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	no ipv6 route distance
Mode	Global Config

ipv6 mtu

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 1280–1500.

Note: The default MTU value for a tunnel interface is 1480. You cannot change this value.

Default	0 or link speed (MTU value (1500))
Format	ipv6 mtu *size*
Mode	Interface Config

no ipv6 mtu

This command resets maximum transmission unit value to default value.

Format	no ipv6 mtu
Mode	Interface Config

ipv6 nd dad attempts

This command sets the number of duplicate address detection probes transmitted on an interface or range of interfaces. 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` *number*
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

This command sets the managed address configuration flag in router advertisements on the interface or range of interfaces. 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 ns-interval

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 {`*`milliseconds`* `| 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

This command sets the other stateful configuration flag in router advertisements sent from the interface.

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

This command sets the transmission interval between router advertisements on the interface or range of interfaces. The *seconds* variable is a number in the range 4–1800 seconds.

Default	600
Format	`ipv6 nd ra-interval-max` *`seconds`*
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

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 *`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` *`lifetime`*
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 ra hop-limit unspecified

This command configures the router to send Router Advertisements on an interface with an unspecified (0) Current Hop Limit value. This tells the hosts on that link to ignore the Hop Limit from this router.

Default	Disable
Format	`ipv6 nd ra hop-limit unspecified`
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	`no ipv6 nd ra hop-limit unspecified`
Mode	Interface Config

ipv6 nd reachable-time

This command sets the router advertisement time to consider a neighbor reachable after neighbor discovery confirmation. Reachable time is specified in milliseconds in a range of 0–4294967295 milliseconds. A value of zero means the time is unspecified by the router. This command can configure a single interface or a range of interfaces.

Default	0
Format	`ipv6 nd reachable-time` *`milliseconds`*
Mode	Interface Config

no ipv6 nd reachable-time

This command means reachable time is unspecified for the router.

Format	`no ipv6 nd reachable-time`
Mode	Interface Config

ipv6 nd router-preference

Use this command to configure default router preferences that the interface advertises in router advertisement messages.

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

This command suppresses router advertisement transmission on an interface or range of interfaces.

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

Use the **`ipv6 nd prefix`** command to configure parameters associated with prefixes the router advertises in its router advertisements. The first optional parameter is the valid lifetime of the router, 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 router 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	`ipv6 nd prefix` *`prefix/prefix_length`* `[{`*`seconds`*` | infinite} {`*`seconds`*` | infinite}] [no-autoconfig off-link]`
Mode	Interface Config

no ipv6 nd prefix

This command sets prefix configuration to default values.

Format	`no ipv6 nd prefix` *`prefix/prefix_length`*
Mode	Interface Config

ipv6 neighbor

Configures a static IPv6 neighbor with the given IPv6 address and MAC address on a routing or host interface.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the *unit/slot/port* format. The *vlan-id* parameter is a number in the range of 1–4093.

Format	`ipv6 neighbor` *ipv6address* {*unit/slot/port* | `vlan` *vland-id*} *macaddr*
Mode	Global Config

Parameter	Definition
ipv6address	The IPv6 address of the neighbor.
unit/slot/port	The *unit/slot/port* for the interface.
vlan-id	The VLAN for the interface.
macaddr	The MAC address for the neighbor.

no ipv6 neighbor

Removes a static IPv6 neighbor with the given IPv6 address on a routing or host interface.

Format	`no ipv6 neighbor` *ipv6address* {*unit/slot/port* | `vlan` *vland-id*}
Mode	Global Config

ipv6 neighbors dynamicrenew

Use this command to automatically renew the IPv6 neighbor entries. Enables/disables the periodic NUD (neighbor unreachability detection) to be run on the existing IPv6 neighbor entries based on the activity of the entries in the hardware. If the setting is disabled, only those entries that are actively used in the hardware are triggered for NUD at the end of STALE timeout of 1200 seconds. If the setting is enabled, periodically 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

Disables automatic renewing of IPv6 neighbor entries.

Format	`no ipv6 neighbors dynamicrenew`
Mode	Global Config

ipv6 nud

Use this command to configure Neighbor Unreachability Detection (NUD). 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.

ipv6 prefix-list (IPv6 routing commands)

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 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 assume if a given prefix does not match any entries of a prefix list. Once a match or deny occurs the router does not go through the rest of the list. A prefix list may be used within a route map to match a route's prefix using the command *match ip address* on page 698.

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` *`list-name`* `{[seq` *`number`*`] {permit | deny}` *`ipv6-prefix/prefix-length`* `[ge` *`length`*`] [le` *`length`*`] | renumber` *`renumber-interval first-statement-number`*`}`
Mode	Global Configuration

Parameter	Description
list-name	The text name of the prefix list. Up to 32 characters.
seq number	(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 *`number`* 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.
ipv6-prefix/prefix-length	Specifies the match criteria for routes being compared to the prefix list statement. The ipv6-prefix can be any valid IP prefix. The length is any IPv6 prefix length from 0 to 32.
ge length	(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.
le length	(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.
renumber	(Optional) Provides the option to renumber the sequence numbers of the IP prefix list statements with a given interval starting from a particular sequence number. The valid range for **`renumber-interval`** is 1–100, and the valid range for *`first-statement-number`* is 1–1000.

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	`no ip prefix-list` *`list-name`* `[[seq` *`number`*`] {permit | deny}` *`network/length`* `[ge` *`length`*`] [le` *`length`*`]]`
Mode	Global Configuration

ipv6 unreachables

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 unreachables`
Mode	Interface Config

no ipv6 unreachables

Use this command to prevent the generation of ICMPv6 Destination Unreachable messages.

Format	`no ipv6 unreachables`
Mode	Interface Config

ipv6 unresolved-traffic

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 50 to 1024 packets per second.

Default	enable
Format	`ipv6 unresolved-traffic rate-limit` *seconds*
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

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 *burst-interval* to zero (0).

Default	*burst-interval* of 1000 msec. *burst-size* of 100 messages
Format	`ipv6 icmp error-interval` *burst-interval* [*burst-size*]
Mode	Global Config

no ipv6 icmp error-interval

Use the **no ipv6 icmp error-interval** 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

Use this command to display the IPv6 status of 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 933.
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 946.
ICMPv6 Rate Limit Burst Size	Shows the number of ICMPv6 error messages that can be sent during one *burst-interval.* For more information, see *ipv6 icmp error-interval* on page 946.
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.

Term	Definition
IPv6 NUD Maximum Unicast Solicits	Shows the maximum number of unicast Neighbor Solicitations sent during NUD (neighbor unreachabililty detection) before switching to multicast Neighbor Solicitations.
IPv6 NUD Maximum Multicast Solicits	Shows the maximum number of multicast Neighbor Solicitations sent during NUD (neighbor unreachabililty 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 unreachabililty 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

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 *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the *unit/slot/port* format. 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. The **tunnel** keyword with the *number* variable specifies the IPv6 tunnel interface and is a number in the range 0–7.

Format	show ipv6 interface [brief | *unit/slot/port* | vlan *vlan-id* | loopback *number* | tunnel *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 *unit/slot/port* 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.
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.

Term	Definition
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 unreachables* on page 946.
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
---------- -------- --------------------------------
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

Use the show ipv6 interface vlan in Privileged EXEC mode to show to show the usability status of IPv6 VLAN interfaces.

Format	`show ipv6 interface vlan` *`vlan-id`* `[prefix]`
Mode	Privileged EXEC User EXEC

Parameter	Description
vlan-id	Valid VLAN ID
prefix	Display IPv6 Interface Prefix Information

show ipv6 dhcp interface

This command displays a list of all IPv6 addresses currently leased from a DHCP server on a specific in-band interface.

The argument *`unit/slot/port`* corresponds to a physical routing interface or VLAN routing interface. The **`vlan`** keyword and *`vland-id`* parameter are used to specify the VLAN

ID of the routing VLAN directly instead of in the *unit/slot/port* format. The *vlan-id* parameter is a number in the range of 1–4093.

Format	show ipv6 dhcp [interface {*unit/slot/port* | vlan *vland-id*}]
Modes	Privileged EXEC

Term	Definition
Mode	Displays whether the specified interface is in Client mode or not.
State	State of the DHCPv6 Client on this interface.The valid values are: INACTIVE, SOLICIT, REQUEST, ACTIVE, RENEW, REBIND, RELEASE.
Server DUID	DHCPv6 Unique Identifier of the DHCPv6 Server on this interface.
T1 Time	The T1 time specified by the DHCPv6 server. After the client has held the address for this length of time, the client tries to renew the lease.
T2 Time	The T2 time specified by the DHCPv6 server. If the lease renewal fails, then when the client has held the lease for this length of time, the client sends a Rebind message to the server.
Interface IAID	An identifier for an identity association chosen by this client.
Leased Address	The IPv6 address leased by the DHCPv6 Server for this interface.
Preferred Lifetime	The preferred lifetime of the IPv6 address, as defined in RFC 2462.
Valid Lifetime	The valid lifetime of the IPv6 address, as defined by RFC 2462.
Renew Time	The time until the client tries to renew the lease
Expiry Time	The time until the address expires.

show ipv6 neighbors

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 *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the *unit/slot/port* format. The *vlan-id* parameter is a number in the range of 1–4093.

The **tunnel** keyword with the *number* variable specifies the IPv6 tunnel interface and is a number in the range 0–7.

Format	show ipv6 neighbor [interface {*unit/slot/port* | vlan *vlan-id* | tunnel *number* | *ipv6-address*]
Mode	Privileged EXEC

Term	Definition
Interface	The interface in *unit/slot/port* 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.

clear ipv6 neighbors

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.

Format	`clear ipv6 neighbors [`*unit/slot/port*`]`
Mode	Privileged EXEC

show ipv6 protocols

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 a protocol is selected on the command line, the display is limited to that protocol.

Format	`show ipv6 protocols [bgp | ospf]`
Mode	Privileged Exec

Parameter	Description
BGP Section:	
Routing Protocol	BGP.
Router ID	The router ID configured for BGP.
Local AS Number	The AS number that the local router is in.
BGP Admin Mode	Whether BGP is globally enabled or disabled.
Maximum Paths	The maximum number of next hops in an internal or external BGP route.

Parameter	Description
Always Compare MED	Whether BGP is configured to compare the MEDs for routes received from peers in different ASs.
Maximum AS Path Length	Limit on the length of AS paths that BGP accepts from its neighbors.
Fast Internal Failover	Whether BGP immediately brings down a iBGP adjacency if the routing table manager reports that the peer address is no longer reachable.
Fast External Failover	Whether BGP immediately brings down an eBGP adjacency if the link to the neighbor goes down.
Distance	The default administrative distance (or route preference) for external, internal, and locally-originated BGP routes. The table that follows lists ranges of neighbor addresses that have been configured to override the default distance with a neighbor-specific distance. If a neighbor's address falls within one of these ranges, routes from that neighbor are assigned the configured distance. If a prefix list is configured, then the distance is only assigned to prefixes from the neighbor that are permitted by the prefix list.
Redistribution	A table showing information for each source protocol (connected, static, rip, and ospf). For each of these sources the distribution list and route-map are shown, as well as the configured metric. Fields which are not configured are left blank. For ospf, an additional line shows the configured ospf match parameters.
Prefix List In	The global prefix list used to filter inbound routes from all neighbors.
Prefix List Out	The global prefix list used to filter outbound routes to all neighbors.
Networks Originated	The set of networks originated through a network command. Those networks that are actually advertised to neighbors are marked "active."
Neighbors	A list of configured neighbors and the inbound and outbound policies configured for each.
OSPFv3 Section:	
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.
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 ............................. BGP
BGP Router ID ................................ 1.1.1.1
Local AS Number .............................. 1
BGP Admin Mode ............................... Enable
Maximum Paths ................................ Internal 1, External 1
Always compare MED ........................... FALSE
Maximum AS Path Length ....................... 75
Fast Internal Failover ....................... Enable
Fast External Failover ....................... Enable
Distance ..................................... Ext 20, Int 200, Local 200

Prefixes Originated:
2005::/64 (active)
3012::/48

Neighbors:
172.20.1.100
Filter List In........................... 1
Filter List Out.......................... 2
Prefix List In........................... PfxList2
Prefix List Out.......................... PfxList3
Route Map In............................. rmapUp
Route Map Out............................ rmapDown


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 route

This command displays the IPv6 routing table The *ipv6-address* specifies a specific IPv6 address for which the best-matching route would be displayed. The *ipv6-prefix/ipv6-prefix-length* specifies a specific IPv6 network for which the matching route would be displayed.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the *unit/slot/port* format. The *vlan-id* parameter is a number in the range of 1–4093.

The *protocol* specifies the protocol that installed the routes. The *protocol* is one of the following keywords: **connected**, **ospf**, or **static**. The **all** keyword specifies that all routes including best and nonbest routes are displayed. Otherwise, only the best routes are displayed.

Note: If you use the **connected** keyword for *protocol*, the **all** option is not available because there are no best or nonbest connected routes.

Format	show ipv6 route [*ipv6-address* [*protocol*] | {{*ipv6-prefix/ipv6-prefix-length* | *unit/slot/port* | vlan *vland-id*} [*protocol*] | *protocol* | summary} [all] | all]
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
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, Truncated
```

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.

Term	Definition
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 would be `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 router, you can configure a static reject route on the router. 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. The reject route added in the RTO is of the type OSPF Inter-Area. Reject routes (routes of REJECT type installed by any protocol) are not redistributed by OSPF/RIP. Reject routes are supported in both OSPFv2 and OSPFv3.

Command example:

```
(NETGEAR Routing) #show ipv6 route

IPv6 Routing Table - 3 entries

Codes: C - connected, S - static
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2

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
OE1 6001::/64 [110/1]
  via fe80::200:42ff:fe7d:2f19,   00h:00m:23s,  0/5
OI 7000::/64 [110/6]
 via fe80::200:4fff:fe35:c8bb,   00h:01m:47s,  0/11
```

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
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2

C    2001:db9:1::/64 [0/0]
      via ::,   0/1
OI   3000::/64 [110/1]
      via fe80::200:e7ff:fe2e:ec3f,   00h:00m:11s,  0/1   T
```

show ipv6 route ecmp-groups

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 preferences

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.
OSPF Intra	Preference of routes within the OSPF area.
OSPF Inter	Preference of routes to other OSPF routes that are outside of the area.
OSPF External	Preference of OSPF external routes.
BGP External	Preference of BGP external routes.
BGP Internal	Preference of routes to other BGP routes that are outside of the area.
BGP Local	Preference of routes within the BGP area.

show ipv6 route summary

This command displays a summary of the state of the routing table. When the optional **`all`** keyword is given, 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 **`all`** 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.
BGP Routes	Total number of routes installed by the BGP protocol.
External	The number of external BGP routes.
Internal	The number of internal BGP routes.
Local	The number of local BGP routes.
OSPF Routes	Total number of routes installed by OSPFv3 protocol.

Term	Definition
Reject Routes	Total number of reject routes installed by all protocols.
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.
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.
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.

Term	Definition
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 Routing) #show ipv6 route summary

Connected Routes.............................. 4
Static Routes................................. 0
6To4 Routes................................... 0
BGP Routes.................................... 10
  External.................................... 0
  Internal.................................... 10
  Local....................................... 0
OSPF Routes................................... 13
  Intra Area Routes........................... 0
  Inter Area Routes........................... 13
  External Type-1 Routes...................... 0
  External Type-2 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

The command resets to zero the IPv6 routing table counters reported in the command *show ipv6 route summary* on page 959. 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

show ipv6 vlan

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 in *unit/slot/port* format 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

Use this command to show traffic and statistics for IPv6 and ICMPv6. Specify a logical, loopback, or tunnel 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 *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the *unit/slot/port* format. 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 [{`*`unit/slot/port`*` | `*`vlan vlan-id`*` | loopback `*`loopback-id`*` | tunnel `*`tunnel-id`*`}]`
Mode	Privileged EXEC

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). Forentities 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.

Term	Definition
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.
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 ipv6IfStatsOutForwDatagrams.
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 ipv6IfStatsOutForwDatagrams 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 ipv6IfIcmpInErrors. 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.

Term	Definition
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.
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.

Term	Definition
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.
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.

clear ipv6 statistics

Use this command to clear IPv6 statistics for all interfaces or for a specific interface, including loopback and tunnel 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	`clear ipv6 statistics [{`*`unit/slot/port`*` | loopback `*`loopback-id`*` | tunnel `*`tunnel-id`*`}]`
Mode	Privileged EXEC

OSPFv3 Commands

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 967
- *OSPFv3 Interface Commands* on page 983
- *OSPFv3 Graceful Restart Commands* on page 988
- *OSPFv3 Stub Router Commands* on page 992
- *OSPFv3 Show Commands* on page 993

Note: OSPFv3 commands are supported on the M5300 and M6100 series switches only.

Global OSPFv3 Commands

ipv6 router ospf

Use this command to enter Router OSPFv3 Config mode.

Format	`router ospf`
Mode	Global Config

area default-cost (OSPFv3)

This command configures the monetary default cost for the stub area. For the *value* argument, you must specify an integer value between 1–16777215.

Format	`area` *`area-id`* `default-cost` *`value`*
Mode	Router OSPFv3 Config

area nssa (OSPFv3)

This command configures the specified *area-id* to function as an NSSA.

Format	`area` *`area-id`* `nssa`
Mode	Router OSPFv3 Config

no area nssa

This command disables nssa from the specified area id.

Format	`no area area-id nssa`
Mode	Router OSPFv3 Config

area nssa default-info-originate (OSPFv3)

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	`area area-id nssa default-info-originate [metric] [comparable | non-comparable]`
Mode	Router OSPFv3 Config

no area nssa default-info-originate (OSPFv3)

This command disables the default route advertised into the NSSA.

Format	`no area area-id nssa default-info-originate [metric] [comparable | non-comparable]`
Mode	Router OSPFv3 Config

area nssa no-redistribute (OSPFv3)

This command configures the NSSA ABR so that learned external routes will not be redistributed to the NSSA.

Format	`area area-id nssa no-redistribute`
Mode	Router OSPFv3 Config

no area nssa no-redistribute (OSPFv3)

This command disables the NSSA ABR so that learned external routes are redistributed to the NSSA.

Format	`no area area-id nssa no-redistribute`
Mode	Router OSPFv3 Config

area nssa no-summary (OSPFv3)

This command configures the NSSA so that summary LSAs are not advertised into the NSSA.

Format	`area` *`area-id`* `nssa no-summary`
Mode	Router OSPFv3 Config

no area nssa no-summary (OSPFv3)

This command disables nssa from the summary LSAs.

Format	`no area` *`area-id`* `nssa no-summary`
Mode	Router OSPFv3 Config

area nssa translator-role (OSPFv3)

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` *`area-id`* `nssa translator-role {always | candidate}`
Mode	Router OSPFv3 Config

no area nssa translator-role (OSPFv3)

This command disables the nssa translator role from the specified area id.

Format	`no area` *`area-id`* `nssa translator-role {always | candidate}`
Mode	Router OSPFv3 Config

area nssa translator-stab-intv (OSPFv3)

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` *`area-id`* `nssa translator-stab-intv` *`stabilityinterval`*
Mode	Router OSPFv3 Config

no area nssa translator-stab-intv (OSPFv3)

This command disables the nssa translator's *stabilityinterval* from the specified area id.

Format	`no area` *area-id* `nssa translator-stab-intv` *stabilityinterval*
Mode	Router OSPFv3 Config

area range (OSPFv3)

Use this command 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	`area` *area-id* `range` *prefix netmask* `{summarylink | nssaexternallink} [advertise | not-advertise] [cost` *cost*`]`
Mode	Router OSPFv3 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	When this keyword is given, the area range is used when summarizing prefixes advertised in type 3 summary LSAs.
nssaexternallink	When this keyword is given, the area range is used when translating type 7 LSAs to type 5 LSAs.
advertise	[Optional] When this keyword is given, the summary prefix is advertised when the area range is active. This is the default.
not-advertise	[Optional] When this keyword is given, neither the summary prefix nor the contained prefixes are advertised when the area range is active. When the not-advertise option is given, any static cost previously configured is removed from the system configuration.
cost	[Optional] If an optional cost is given, 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

The **`no area range`** command deletes a summary prefix or removes a static cost.

Format	`no area` *area-id* `range` *prefix netmask* `{summarylink | nssaexternallink} cost`
Mode	Router OSPFv3 Config

area stub (OSPFv3)

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	`area` *`area-id`* `stub`
Mode	Router OSPFv3 Config

no area stub

This command deletes a stub area for the specified area ID.

Format	`no area` *`area-id`* `stub`
Mode	Router OSPFv3 Config

area stub no-summary (OSPFv3)

This command disables the import of Summary LSAs for the stub area identified by *`area-id`*.

Default	enabled
Format	`area` *`area-id`* `stub no-summary`
Mode	Router OSPFv3 Config

no area stub no-summary

This command sets the Summary LSA import mode to the default for the stub area identified by *`area-id`*.

Format	`no area` *`area-id`* `stub summarylsa`
Mode	Router OSPFv3 Config

area virtual-link (OSPFv3)

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` *`area-id`* `virtual-link` *`neighbor`*
Mode	Router OSPFv3 Config

no area virtual-link

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	`no area` *area-id* `virtual-link` *neighbor*
Mode	Router OSPFv3 Config

area virtual-link dead-interval (OSPFv3)

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` *area-id* `virtual-link` *neighbor* `dead-interval` *seconds*
Mode	Router OSPFv3 Config

no area virtual-link dead-interval

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` *area-id* `virtual-link` *neighbor* `dead-interval`
Mode	Router OSPFv3 Config

area virtual-link hello-interval (OSPFv3)

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	`area` *area-id* `virtual-link` *neighbor* `hello-interval` *seconds*
Mode	Router OSPFv3 Config

no area virtual-link hello-interval

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	`no area` *area-id* `virtual-link` *neighbor* `hello-interval`
Mode	Router OSPFv3 Config

area virtual-link retransmit-interval (OSPFv3)

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	`area` *area-id* `virtual-link` *neighbor* `retransmit-interval` *seconds*
Mode	Router OSPFv3 Config

no area virtual-link retransmit-interval

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	`no area` *area-id* `virtual-link` *neighbor* `retransmit-interval`
Mode	Router OSPFv3 Config

area virtual-link transmit-delay (OSPFv3)

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	`area` *area-id* `virtual-link` *neighbor* `transmit-delay` *seconds*
Mode	Router OSPFv3 Config

no area virtual-link transmit-delay

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	`no area` *area-id* `virtual-link` *neighbor* `transmit-delay`
Mode	Router OSPFv3 Config

auto-cost (OSPFv3)

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 (ref_bw / 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	`auto-cost reference-bandwidth` *mbps*
Mode	Router OSPFv3 Config

no auto-cost reference-bandwidth (OSPFv3)

Use this command to set the reference bandwidth to the default value.

Format	`no auto-cost reference-bandwidth`
Mode	Router OSPFv3 Config

clear ipv6 ospf

Use this command to disable and re-enable OSPF.

Format	`clear ipv6 ospf`
Mode	Privileged EXEC

clear ipv6 ospf configuration

Use this command to reset the OSPF configuration to factory defaults.

Format	`clear ipv6 ospf configuration`
Mode	Privileged EXEC

clear ipv6 ospf counters

Use this command to reset global and interface statistics.

Format	`clear ipv6 ospf counters`
Mode	Privileged EXEC

clear ipv6 ospf neighbor

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	`clear ipv6 ospf neighbor [`*neighbor-id*`]`
Mode	Privileged EXEC

clear ipv6 ospf neighbor interface

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 *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the *unit/slot/port* format. 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	`clear ipv6 ospf neighbor interface [`*unit/slot/port* `| vlan` *vland-id*`] [`*neighbor-id*`]`
Mode	Privileged EXEC

clear ipv6 ospf redistribution

Use this command to flush all self-originated external LSAs. Reapply the redistribution configuration and re-originate prefixes as necessary.

Format	`clear ipv6 ospf redistribution`
Mode	Privileged EXEC

default-information originate (OSPFv3)

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` *`metric`*`] [metric-type {1 | 2}]`
Mode	Router OSPFv3 Config

no default-information originate (OSPFv3)

This command is used to control the advertisement of default routes.

Format	`no default-information originate [`*`metric`*`] [`*`metric-type`*`]`
Mode	Router OSPFv3 Config

default-metric (OSPFv3)

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` *`metric`*
Mode	Router OSPFv3 Config

no default-metric (OSPFv3)

This command is used to set a default for the metric of distributed routes.

Format	`no default-metric`
Mode	Router OSPFv3 Config

distance ospf (OSPFv3)

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` *preference* `| inter-area` *preference* `| external` *preference*`}`
Mode	Router OSPFv3 Config

no distance ospf

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 (OSPFv3)

This command resets the default administrative mode of OSPF in the router (active).

Default	enabled
Format	`enable`
Mode	Router OSPFv3 Config

no enable (OSPFv3)

This command sets the administrative mode of OSPF in the router to inactive.

Format	`no enable`
Mode	Router OSPFv3 Config

exit-overflow-interval (OSPFv3)

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` *`seconds`*
Mode	Router OSPFv3 Config

no exit-overflow-interval

This command configures the default exit overflow interval for OSPF.

Format	`no exit-overflow-interval`
Mode	Router OSPFv3 Config

external-lsdb-limit (OSPFv3)

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 it 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	`external-lsdb-limit` *`limit`*
Mode	Router OSPFv3 Config

no external-lsdb-limit

This command configures the default external LSDB limit for OSPF.

Format	`no external-lsdb-limit`
Mode	Router OSPFv3 Config

maximum-paths (OSPFv3)

This command sets the number of paths that OSPF can report for a given destination where *`maxpaths`* is platform dependent.

Default	4
Format	`maximum-paths` *`maxpaths`*
Mode	Router OSPFv3 Config

no maximum-paths

This command resets the number of paths that OSPF can report for a given destination back to its default value.

Format	`no maximum-paths`
Mode	Router OSPFv3 Config

passive-interface default (OSPFv3)

Use this command to enable global passive mode by default for all interfaces. It overrides any interface level passive mode. OSPF shall not form adjacencies over a passive interface.

Default	disabled
Format	`passive-interface default`
Mode	Router OSPFv3 Config

no passive-interface default

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 OSPFv3 Config

passive-interface (OSPFv3)

Use this command to set the interface or tunnel as passive.

The argument *`unit/slot/port`* corresponds to a physical routing interface or VLAN routing interface. The **`vlan`** keyword and *`vland-id`* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the *`unit/slot/port`* format. The *`vlan-id`* parameter is a number in the range of 1–4093. You can also use the tunnel **`keyword`** and *`tunnel-id`* argument.

Using these arguments overrides the global passive mode that is effective on the interface or tunnel.

Default	disabled
Format	`passive-interface {`*`unit/slot/port`* `|` *`vlan vland-id`* `| tunnel` *`tunnel-id`*`}`
Mode	Router OSPFv3 Config

no passive-interface

Use this command to set the interface, VLAN, or tunnel as nonpassive. It overrides the global passive mode that is currently effective on the interface or tunnel.

Format	`no passive-interface {`*`unit/slot/port`* `|` *`vlan vlan-id`* `|` `tunnel` *`tunnel-id`*`}`
Mode	Router OSPFv3 Config

redistribute (OSPFv3)

This command configures the OSPFv3 protocol to allow redistribution of routes from the specified source protocol/routers. The *`metric`* argument can be a number in the range 0–16777214. The metric type can be 1 or 2. The tag argument can be a number in the range 0–4294967295.

Default	metric—unspecified type—2 tag—0
Format	`redistribute {static | connected} [metric` *`metric`*`] [metric-type {1 | 2}] [tag` *`tag`*`]`
Mode	Router OSPFv3 Config

no redistribute

This command configures OSPF protocol to prohibit redistribution of routes from the specified source protocol/routers.

Format	`no redistribute {static | connected} [metric] [metric-type] [tag]`
Mode	Router OSPFv3 Config

router-id (OSPFv3)

This command sets a 4-digit dotted-decimal number uniquely identifying the router ospf id. The *`ipaddress`* is a configured value.

Format	`router-id` *`ipaddress`*
Mode	Router OSPFv3 Config

timers pacing lsa-group (OSPFv3)

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.

seconds is 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	`timers pacing lsa-group` *seconds*
Mode	Router OSPFv3 Config

no timers pacing lsa-group

This command returns the LSA Group Pacing parameter to the factory default value of 60 seconds.

Format	`no timers pacing lsa-group`
Mode	Router OSPFv3 Config

timers throttle spf

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	*spf-start* = 2000 ms *spf-hold* = 5000 ms *spf-maximum* = 5000 ms
Format	`timers throttle spf` *spf-start spf-hold spf-maximum*
Mode	Router OSPFv3 Config

Parameter	Description
spf-start	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.

Parameter	Description
spf-hold	Indicates the initial SPF wait interval in milliseconds. Value range is 1 to 600000 milliseconds.
spf-maximum	Indicates the maximum SPF wait interval in milliseconds. Value range is 1 to 600000 milliseconds.

no timers throttle spf

This command returns the SPF throttling parameters to the factory default values.

Format	`no timers throttle spf`
Mode	Router OSPFv3 Config

trapflags (OSPFv3)

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 14. Trapflag 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 the 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	`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}}`
Mode	Router OSPFv3 Config

no trapflags

Use this command to revert to the default reference bandwidth.

- To disable the 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 | 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}}`
Mode	Router OSPFv3 Config

OSPFv3 Interface Commands

ipv6 ospf area

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 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` *`area-id`*
Mode	Interface Config

ipv6 ospf cost

This command configures the cost on an OSPF interface or range of interfaces. The *`cost`* parameter has is in the range of 1 to 65535.

Default	10
Format	`ipv6 ospf cost` *`cost`*
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

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` *`seconds`*
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

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	`ipv6 ospf hello-interval` *seconds*
Mode	Interface Config

no ipv6 ospf hello-interval

This command sets the default OSPF hello interval for the specified interface.

Format	`no ipv6 ospf hello-interval`
Mode	Interface Config

ipv6 ospf link-lsa-suppression

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	`ipv6 ospf link-lsa-suppression`
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	`no ipv6 ospf link-lsa-suppression`
Mode	Privileged EXEC

ipv6 ospf mtu-ignore

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	`ipv6 ospf mtu-ignore`
Mode	Interface Config

no ipv6 ospf mtu-ignore

This command enables the OSPF MTU mismatch detection.

Format	`no ipv6 ospf mtu-ignore`
Mode	Interface Config

ipv6 ospf network

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. Similarly, tunnel interfaces default to point-to-point. 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. It is normally not useful to set a tunnel to OSPF network type broadcast.

Default	broadcast
Format	`ipv6 ospf network {broadcast | point-to-point}`
Mode	Interface Config

no ipv6 ospf network

This command sets the interface type to the default value.

Format	`no ipv6 ospf network {broadcast | point-to-point}`
Mode	Interface Config

ipv6 ospf prefix-suppression

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	`ipv6 ospf prefix-suppression [disable]`
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. Not configuring the command is not equal to disabling interface level prefix-suppression.

Format	`no ipv6 ospf prefix-suppression`
Mode	Interface Config

ipv6 ospf priority

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	`ipv6 ospf priority` *`priority`*
Mode	Interface Config

no ipv6 ospf priority

This command sets the default OSPF priority for the specified router interface.

Format	`no ipv6 ospf priority`
Mode	Interface Config

ipv6 ospf retransmit-interval

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` *seconds*
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

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. 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` *seconds*
Mode	Interface Config

no ipv6 ospf transmit-delay

This command sets the default OSPF Transit Delay for the specified interface.

Format	`no ipv6 ospf transmit-delay`
Mode	Interface Config

OSPFv3 Graceful Restart Commands

The OSPFv3 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 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 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 (OSPFv3)

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 (OSPFv3)

Use this command to disable graceful restart for all restarts.

Format	`no nsf [ietf] [planned-only]`
Modes	Router OSPFv3 Config

nsf restart-interval (OSPFv3)

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` *seconds*
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 nsfrestart-interval (OSPFv3)

Use this command to revert the grace period to its default value.

Format	`no [ietf] nsf restart-interval`
Modes	Router OSPFv3 Config

nsf helper (OSPFv3)

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	`nsf helper [planned-only]`
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 (OSPFv3)

Use this command to disable helpful neighbor functionality for OSPF.

Format	`no nsf helper`
Modes	Router OSPFv3 Config

nsf ietf helper disable (OSPFv3)

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	`nsf ietf helper disable`
Modes	Router OSPFv3 Config

nsf helper strict-lsa-checking (OSPFv3)

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	`nsf [ietf] helper strict-lsa-checking`
Modes	Router OSPFv3 Config

Parameter	Description
ietf	This keyword is accepted but not required.

no nsf [ietf] helper strict-lsa-checking (OSPFv3)

Use this command to allow OSPF to continue as a helpful neighbor in spite of topology changes.

Default	Enabled.
Format	`nsf [ietf] helper strict-lsa-checking`
Modes	Router OSPFv3 Config

OSPFv3 Stub Router Commands

max-metric router-lsa (OSPFv3 Router Configuration)

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 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 router to enter stub router mode on startup (max-metric router-lsa on-startup), and then enter max-metric router lsa, there is no change. If OSPFv3 is administratively in stub router mode (the max-metric router-lsa command has been given), and you configure OSPFv3 to enter stub router mode on startup (max-metric router-lsa on-startup), 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	`max-metric router-lsa [on-startup` *`seconds`*`] [summary-lsa {metric}]` `max-metric router-lsa [external-lsa [`*`max-metric-value`*`]] [inter-area-lsas [`*`max-metric-value`*`]] [on-startup` *`seconds`*`] [summary-lsa [`*`max-metric-value`*`]]`
Mode	OSPFv3 Router Configuration

Parameter	Description
external-lsa	(Optional) Sends the maximum metric values for external LSAs. *`max-metric-value`* is the maximum metric value to use for LSAs. The range is 1 to 16777215 (0xFFFFFF). The default value is 16711680 (0xFF0000).
inter-area-lsas	(Optional) Sends the maximum metric values for Inter-Area-Router LSAs. *`max-metric-value`* is the maximum metric value to use for LSAs. The range is 1 to 16777215 (0xFFFFFF). The default value is 16711680 (0xFF0000).
on-startup	(Optional) Starts OSPF in stub router mode. *`seconds`* 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. *`max-metric-value`* is the maximum metric value to use for LSAs. The range is 1 to 16777215 (0xFFFFFF). The default value is 16711680 (0xFF0000).

no max-metric router-lsa

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, issue the command **no max-metric router-lsa on-startup**. The command **no max-metric router-lsa** with the **external-lsa**, **inter-area-lsas**, **on-startup**, or **summary-lsa** option causes OSPF to send summary LSAs with metrics computed using normal procedures.

Format	`no max-metric router-lsa [external-lsa] [inter-area-lsas] [on-startup] [summary-lsa]`
Mode	OSPFv3 Router Configuration

clear ipv6 ospf stub-router

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 it if is in stub router mode at startup. This command has no effect if OSPF is configured to be in stub router mode permanently.

Format	`clear ipv6 ospf stub-router`
Mode	Privileged EXEC

OSPFv3 Show Commands

show ipv6 ospf

This command displays information relevant to the OSPF router.

Format	`show ipv6 ospf`
Mode	Privileged EXEC User 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.
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 given 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

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 at any given time.
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.

Term	Definition
Distribute-List	The access list used to filter redistributed routes.
Prefix-suppression	Displays whether prefix-suppression is enabled or disabled on the given 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

This command displays the internal OSPFv3 routes to reach Area Border Routers (ABR). This command takes no options.

Format	`show ipv6 ospf abr`
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.

Term	Definition
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

This command displays information about the area. The *area-id* identifies the OSPF area that is being displayed.

Format	`show ipv6 ospf area` *area-id*
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 a 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.

Term	Definition
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.

show ipv6 ospf asbr

This command displays the internal OSPFv3 routes to reach Autonomous System Boundary Routers (ASBR). This command takes no options.

Format	`show ipv6 ospf asbr`
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

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	`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}]`
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

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	`show ipv6 ospf database database-summary`
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

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 directly instead of in a *unit/slot/port* format. 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. You can use the **tunnel** keyword and *tunnel-id* argument to specify a tunnel interface.

Format	`show ipv6 ospf interface {`*`unit/slot/port`* `|` *`vlan vlan-id`* `|` `loopback` *`loopback-id`* `|` `tunnel` *`tunnel-id`*`}`
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.

Term	Definition
OSPF Area ID	The area ID associated with this interface.
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 given 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

This command displays brief information for the physical interface or virtual interface tables.

Format	`show ipv6 ospf interface brief`
Modes	Privileged EXEC User EXEC

Term	Definition
Interface	*unit/slot/port*
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

This command displays the statistics for a specific interface. The command displays information only if OSPF is enabled.

Format	`show ipv6 ospf interface stats` *unit/slot/port*
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 AllDrRouters 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 (OSPF)* on page 760 lists the number of OSPF packets of each type sent and received on the interface.

show ipv6 ospf lsa-group

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.

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

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

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 or tunnel, only the information for that interface or tunnel 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 directly instead of in a *unit/slot/port* format. The *vlan-id* can be a number from 1–4093. You can also use the **tunnel** keyword with the *tunnel-id* argument to specify a tunnel.

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* `| tunnel` *tunnel-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 *unit/slot/port* 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 is to decide which router is the master and to decide upon the initial DD sequence number. • Exchange - the router is describing its entire link state database by sending Database Description packets to the neighbor. • Full - the neighboring routers are fully adjacent and they will now 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—This router is acting as a helpful neighbor to the specified router. • Not Helping—This 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 *unit/slot/port* 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

This command displays the set of OSPFv3 area ranges configured for a given area.

Format	`show ipv6 ospf range` *area-id*
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

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
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

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

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.
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

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.

Note: DHCPv6 commands are supported on the M5300 and M6100 series switches only.

service dhcpv6

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

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.

`rapid-commit` 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 server

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 {*pool-name* | automatic} [rapid-commit] [preference *pref-value*]
Mode	Interface Config

ipv6 dhcp relay destination

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 (*unit/slot/port*) to 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-ifid**, 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	ipv6 dhcp relay {destination [*relay-address*] interface [*relay-interface*]| interface [*relay-interface*]} [remote-id {duid-ifid | *user-defined-string*}]
Mode	Interface Config

ipv6 dhcp pool

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	`ipv6 dhcp pool` *`pool-name`*
Mode	Global Config

no ipv6 dhcp pool

This command removes the specified DHCPv6 pool.

Format	`no ipv6 dhcp pool` *`pool-name`*
Mode	Global Config

address prefix (IPv6)

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	`address prefix` *`ipv6-prefix`* `[lifetime {`*`valid-lifetime preferred-lifetime`* `| infinite}]`
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.
valid-lifetime	The amount of time, in seconds, the prefix remains valid for the requesting router to use. The range is from 60 through 4294967294. The *`preferred-lifetime`* value cannot exceed the *`valid-lifetime`* value.
preferred-lifetime	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 *`preferred-lifetime`* value cannot exceed the *`valid-lifetime`* 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
```

domain-name (IPv6)

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	`domain-name` *`dns-domain-name`*
Mode	IPv6 DHCP Pool Config

no domain-name

This command removes dhcpv6 domain name from dhcpv6 pool.

Format	`no domain-name` *`dns-domain-name`*
Mode	IPv6 DHCP Pool Config

dns-server (IPv6)

This command sets the ipv6 DNS server address which is provided to dhcpv6 client by dhcpv6 server. The DNS server address is configured for stateless server support. DHCPv6 pool can have multiple number of domain names with a maximum of 8.

Format	`dns-server` *`dns-server-address`*
Mode	IPv6 DHCP Pool Config

no dns-server

This command removes DHCPv6 server address from DHCPv6 server.

Format	`no dns-server` *`dns-server-address`*
Mode	IPv6 DHCP Pool Config

prefix-delegation (IPv6)

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.
- preferred lifetime is the preferred lifetime for the delegated prefix in *seconds*, in a range from 0–4294967295 seconds.

Default	**valid-lifetime** *seconds*: 2592000 **preferred-lifetime** *seconds*: 604800
Format	prefix-delegation *prefix/prefixlength duid* [name *hostname*] [valid-lifetime *seconds*] [preferred-lifetime *seconds*]
Mode	IPv6 DHCP Pool Config

no prefix-delegation

This command deletes a specific prefix-delegation client.

Format	no prefix-delegation *prefix/prefix-delegation duid*
Mode	IPv6 DHCP Pool Config

show ipv6 dhcp

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

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.
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

This command displays DHCPv6 information for all relevant interfaces or 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 directly instead of in a *unit/slot/port* format. The *vlan-id* can be a number from 1–4093.

If you specify an interface, you can use the optional `statistics` parameter to view statistics for the specified interface.

Format	`show ipv6 dhcp interface {`*`unit/slot/port`* `| vlan` *`vlan-id`*`} [statistics]`
Mode	Privileged EXEC

Term	Definition
IPv6 Interface	The interface name in *`unit/slot/port`* format.
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.
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 in *`unit/slot/port`* format.
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 1016 for information about the output.

show ipv6 dhcp binding

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.

Term	Definition
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.
Valid Lifetime	Valid lifetime in seconds for delegated prefix.
Preferred Lifetime	Preferred lifetime in seconds for delegated prefix.

show ipv6 dhcp pool

This command displays configured DHCP pool.

Format	`show ipv6 dhcp pool` *`pool-name`*
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 network ipv6 dhcp statistics

This command displays the statistics of the DHCPv6 client running on the network management interface.

Format	`show network ipv6 dhcp statistics`
Mode	Privileged EXEC User EXEC

Field	Description
DHCPv6 Advertisement Packets Received	The number of DHCPv6 Advertisement packets received on the network interface.
DHCPv6 Reply Packets Received	The number of DHCPv6 Reply packets received on the network interface.
Received DHCPv6 Advertisement Packets Discarded	The number of DHCPv6 Advertisement packets discarded on the network interface.
Received DHCPv6 Reply Packets Discarded	The number of DHCPv6 Reply packets discarded on the network interface.
DHCPv6 Malformed Packets Received	The number of DHCPv6 packets that are received malformed on the network interface.
Total DHCPv6 Packets Received	The total number of DHCPv6 packets received on the network interface.
DHCPv6 Solicit Packets Transmitted	The number of DHCPv6 Solicit packets transmitted on the network interface.
DHCPv6 Request Packets Transmitted	The number of DHCPv6 Request packets transmitted on the network interface.
DHCPv6 Renew Packets Transmitted	The number of DHCPv6 Renew packets transmitted on the network interface.
DHCPv6 Rebind Packets Transmitted	The number of DHCPv6 Rebind packets transmitted on the network interface.
DHCPv6 Release Packets Transmitted	The number of DHCPv6 Release packets transmitted on the network interface.
Total DHCPv6 Packets Transmitted	The total number of DHCPv6 packets transmitted on the network interface.

Command example:

```
(admin)#show network 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
```

show serviceport ipv6 dhcp statistics

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.
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:

```
(admin)#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

Use this command to clear DHCPv6 statistics for all interfaces or for a specific interface. Use the *unit/slot/port* parameter to specify the interface.

Format	`clear ipv6 dhcp {statistics | interface` *unit/slot/port* `statistics}`
Mode	Privileged EXEC

clear ipv6 dhcp binding

This command deletes an automatic address binding from the DHCP server database. *address* is a valid IPv6 address.

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 specified, 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	`clear ipv6 dhcp binding [`*ipv6-address*`]`
Mode	Privileged EXEC

clear network ipv6 dhcp statistics

Use this command to clear the DHCPv6 statistics on the network management interface.

Format	`clear network ipv6 dhcp statistics`
Mode	Privileged EXEC

clear serviceport ipv6 dhcp statistics

Use this command to clear the DHCPv6 client statistics on the service port interface.

Format	`clear serviceport ipv6 dhcp statistics`
Mode	Privileged EXEC

DHCPv6 Snooping Configuration Commands

This section describes commands you use to configure IPv6 DHCP Snooping.

ipv6 dhcp snooping

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

Use this command to enable DHCP Snooping on a list of comma-separated VLAN ranges.

Default	disabled
Format	`ipv6 dhcp snooping vlan` *`vlan-list`*
Mode	Global Config

no ipv6 dhcp snooping vlan

Use this command to disable DHCP Snooping on VLANs.

Format	`no ipv6 dhcp snooping vlan` *`vlan-list`*
Mode	Global Config

ipv6 dhcp snooping verify mac-address

Use this command to enable verification of the source MAC address with the client hardware address in the received DCHP 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

Use this command to configure the persistent location of the DHCP Snooping database. This can be local or a remote file on a given IP machine.

Default	local
Format	`ipv6 dhcp snooping database {local | tftp://`*`hostIP/filename`*`}`
Mode	Global Config

ip dhcp snooping database write-delay (DHCPv6)

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` *`seconds`*
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

Use this command to configure static DHCP Snooping binding.

Format	`ipv6 dhcp snooping binding` *`mac-address`* `vlan` *`vlan-id ipaddress`* `interface` *`interface-id`*
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` *`mac-address`*
Mode	Global Config

ipv6 dhcp snooping trust

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

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

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.

Default	disabled (no limit)
Format	`ipv6 dhcp snooping limit {rate` *`pps`* `[`*`burst interval seconds`*`]}`
Mode	Interface Config

no ipv6 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	`no ipv6 dhcp snooping limit`
Mode	Interface Config

ipv6 verify source

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	`ipv6 verify source {port-security}`
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	`no ipv6 verify source`
Mode	Interface Config

ipv6 verify binding

Use this command to configure static IPv6 source guard (IPv6SG) entries.

Format	`ipv6 verify binding` *`mac-address`* `vlan` *`vlan-id ipv6-address`* `interface` *`interface-id`*
Mode	Global Config

no ipv6 verify binding

Use this command to remove the IPv6SG static entry from the IPv6SG database.

Format	`no ipv6 verify binding` *`mac-address`* `vlan` *`vlan-id ipv6-address`* `interface` *`interface-id`*
Mode	Global Config

show ipv6 dhcp snooping

Use this command to display the DHCP Snooping global configurations and per port configurations.

Format	`show ipv6 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 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

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 DCHP snooping.
- **`interface`** *`unit/slot/port`*. Restrict the output based on a specific interface.
- *`vlan-id`*. Restrict the output based on a VLAN.

Format	`show ipv6 dhcp snooping binding [static | dynamic] [interface` *`unit/slot/port`*`] [`*`vlan-id`*`]`
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.
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

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:/sai1.txt
write-delay:  5000
```

show ipv6 dhcp snooping interfaces

Use this command to show the DHCP Snooping status of all interfaces or a specified interface.

Format	`show ipv6 dhcp snooping interfaces [interface` *`unit/slot/port`*`]`
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) #show ipv6 dhcp snooping interfaces
Interface    Trust State   Rate Limit    Burst Interval
                              (pps)         (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    Burst Interval
                              (pps)         (seconds)
-----------   ----------    -----------   --------------
1/0/1             Yes           151
```

show ipv6 dhcp snooping statistics

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 *`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 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   Client Ifc   DHCP Server
               Failures     Mismatch    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

Use this command to clear all DHCPv6 Snooping bindings on all interfaces or on a specific interface.

Format	`clear ipv6 dhcp snooping binding [interface` *`unit/slot/port`*`]`
Mode	Privileged EXEC User EXEC

clear ipv6 dhcp snooping statistics

Use this command to clear all DHCPv6 Snooping statistics.

Format	`clear ipv6 dhcp snooping statistics`
Mode	Privileged EXEC User EXEC

show ipv6 verify

Use this command to display the IPv6 configuration on a specified interface in the *`unit/slot/port`* format.

Format	`show ipv6 verify` *`unit/slot/port`*
Mode	Privileged EXEC User EXEC

Term	Definition
Interface	Interface address in *`unit/slot/port`* 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 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

Use this command to display the IPv6SG configurations on all ports. If the **interface** option is specified, the output is restricted to the specified *unit/slot/port* argument.

Format	show ipv6 verify source [interface *unit/slot/port*]
Mode	Privileged EXEC User EXEC

Term	Definition
Interface	Interface address in *unit/slot/port* 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

Use this command to display the IPv6SG bindings.

Format	show ipv6 source binding [dhcp-snooping | static] [interface *unit/slot/port*] [*vlan-id*]
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.

Term	Definition
VLAN	VLAN for the entry.
Interface	IP address of the interface in *unit/slot/port* 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
```

Quality of Service Commands

14

This chapter describes the Quality of Service (QoS) commands available in the NETGEAR Managed Switch CLI. 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

This command maps an 802.1p priority to an internal traffic class. The *userpriority* values can range from 0-7. The *trafficclass* values range from 0-6, although the actual number of available traffic classes depends on the platform.

Format	`classofservice dot1p-mapping` *userpriority trafficclass*
Modes	Global Config Interface Config

no classofservice dot1p-mapping

This command maps each 802.1p priority to its default internal traffic class value.

Format	`no classofservice dot1p-mapping`
Modes	Global Config Interface Config

classofservice ip-dscp-mapping

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 *trafficclass* values can range from 0-6, although the actual number of available traffic classes depends on the platform.

Format	`classofservice ip-dscp-mapping` *ipdscp trafficclass*
Mode	Global Config

no classofservice ip-dscp-mapping

This command maps each IP DSCP value to its default internal traffic class value.

Format	`no classofservice ip-dscp-mapping`
Mode	Global Config

classofservice trust

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

This command specifies the minimum transmission bandwidth (*bw*) guarantee for each interface queue on an interface, a range of interfaces, or all interfaces. The total number of queues supported per interface is platform specific. 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` *`bw-0 bw-1 … bw-n`*
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

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	`cos-queue random-detect` *`queue-id-1`* [*`queue-id-2 … queue-id-n`*]
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 and 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	`no cos-queue random-detect` *`queue-id-1`* [*`queue-id-2 … queue-id-n`*]
Modes	Global Config Interface Config

cos-queue strict

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.

Format	`cos-queue strict` *`queue-id-1`* [*`queue-id-2 … queue-id-n`*]
Modes	Global Config Interface Config

no cos-queue strict

This command restores the default weighted scheduler mode for each specified queue.

Format	`no cos-queue strict` *`queue-id-1`* [*`queue-id-2 … queue-id-n`*]
Modes	Global Config Interface Config

random-detect

This command is used to enable WRED for the interface as a whole, and is only available when per-queue WRED activation control is not supported by the device Specific WRED parameters are configured using the **`random-detect queue-parms`** and the **`random-detect exponential-weighting-constant`** commands.

Format	`random-detect`
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. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

no random-detect

Use this command to disable WRED, thereby restoring the default tail drop operation for all queues on the interface.

Format	`no random-detect`
Modes	Global Config Interface Config

random-detect exponential weighting-constant

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	`random-detect exponential-weighting-constant` *`number`*
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	`no random-detect exponential-weighting-constant`
Modes	Global Config Interface Config

random-detect queue-parms

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).

Format	`random-detect queue-parms` *`queue-id-1`* `[`*`queue-id-2 … queue-id-n`*`] min-thresh` *`thresh-prec-1 … thresh-prec-n`* `max-thresh` *`thresh-prec-1 … thresh-prec-n`* `drop-probability` *`prob-prec-1 … prob-prec-n`*
Modes	Global Config Interface Config

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 3-color system, four of each parameter specified: green TCP, yellow TCP, red TCP, and non-TCP, respectively.

Term	Definition
min-thresh	The minimum threshold the queue depth (as a percentage) where WRED starts marking and dropping traffic.
max-thresh	The maximum threshold is the queue depth (as a percentage) above which WRED marks / drops all traffic.
drop-probability	The percentage probability that WRED will mark/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).

no random-detect queue-parms

Use this command to set the WRED configuration back to the default.

Format	`no random-detect queue-parms` *`queue-id-1`* `[`*`queue-id-2 … queue-id-n`*`]`
Modes	Global Config Interface Config

traffic-shape

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	`traffic-shape` *`bw`*
Modes	Global Config Interface Config

no traffic-shape

This command restores the interface shaping rate to the default value.

Format	`no traffic-shape`
Modes	Global Config Interface Config

show classofservice dot1p-mapping

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 418.

Format	`show classofservice dot1p-mapping [`*`unit/slot/port`*`]`
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

This command displays the current IP DSCP mapping to internal traffic classes for the global configuration settings.

Format	`show classofservice ip-dscp-mapping`
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 ip-precedence-mapping

This command displays the current IP Precedence 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 IP Precedence mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format	`show classofservice ip-precedence-mapping [`*unit/slot/port*`]`
Mode	Privileged EXEC

Term	Definition
IP Precedence	The IP Precedence value.
Traffic Class	The traffic class internal queue identifier to which the IP Precedence value is mapped.

show classofservice trust

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.

Format	`show classofservice trust [`*unit/slot/port*`]`
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

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.

Format	`show interfaces cos-queue [unit/slot/port]`
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 *unit/slot/port* 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

This command displays the global WRED settings for each CoS queue. If you specify the *unit/slot/port*, the command displays the WRED settings for each CoS queue on the specified interface.

Format	`show interfaces random-detect [unit/slot/port]`
Mode	Privileged EXEC

Term	Definition
Queue ID	An interface supports n queues numbered 0 to (n-1). The specific n value is platform dependent.
WRED Minimum Threshold	The configured minimum threshold 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 / drops all traffic.
WRED Drop Probability	The configured percentage probability that WRED will mark/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).

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 given 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

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: Once 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

This command defines a DiffServ class of type match-all. When used without any match condition, this command enters the class-map mode. The *class-map-name* is a case sensitive alphanumeric string from 1 to 31 characters uniquely identifying an existing DiffServ class.

Note: The **class-map-name** default is reserved. Do not use it.

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.

Note: 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.

Note: 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.

Format	class-map match-all *class-map-name* [ipv4 | ipv6]
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	`no class-map` *`class-map-name`*
Mode	Global Config

class-map rename

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` *`class-map-name new-class-map-name`*
Mode	Global Config

match ethertype

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. Use the **`not`** option to negate the match condition.

Format	`match [not] ethertype {`*`keyword`*` | custom `*`range`*`}`
Mode	Class-Map Config Ipv6-Class-Map Config

match any

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class. Use the **`not`** option to negate the match condition.

Default	none
Format	`match [not] any`
Mode	Class-Map Config Ipv6-Class-Map Config

match class-map

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 *refclassname*
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* fails.
- 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 *refclassname*
Mode	Class-Map Config Ipv6-Class-Map Config

match cos

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. Use the **not** option to negate the match condition.

Default	none
Format	`match [not] cos` *`value`*
Mode	Class-Map Config Ipv6-Class-Map Config

match secondary-cos

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. Use the **`not`** option to negate the match condition.

Default	none
Format	`match [not] secondary-cos` *`value`*
Mode	Class-Map Config Ipv6-Class-Map Config

match destination-address mac

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). Use the **`not`** option to negate the match condition.

Default	none
Format	`match [not] destination-address mac` *`macaddr macmask`*
Mode	Class-Map Config Ipv6-Class-Map Config

match dstip

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. Use the **`not`** option to negate the match condition.

Default	none
Format	`match [not] dstip` *`ipaddr ipmask`*
Mode	Class-Map Config

match dstip6

This command adds to the specified class definition a match condition based on the destination IPv6 address of a packet. Use the **not** option to negate the match condition.

Default	none
Format	`match [not] dstip6 destination-ipv6-prefix/prefix-length`
Mode	Ipv6-Class-Map Config

match dstl4port

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. Use the **not** option to negate the match condition.

Default	none
Format	`match [not] dstl4port {portkey | port-number}`
Mode	Class-Map Config Ipv6-Class-Map Config

match ip dscp

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**. Use the **not** option to negate the match condition.

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 [not] ip dscp dscpval`
Mode	Class-Map Config Ipv6-Class-Map Config

match ip precedence

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. Use the **not** option to negate the match condition.

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 [not] ip precedence value`
Mode	Class-Map Config

match ip tos

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). Use the **not** option to negate the match condition.

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 the user complete control when specifying which bits of the IP Service Type field are checked.

Default	none
Format	`match [not] ip tos tosbits tosmask`
Mode	Class-Map Config

match ip6flowlbl

Use this command to enter an IPv6 flow label value. Use the **not** option to negate the match condition. The *value* argument can be in the range of 0–1048575.

Default	none
Format	`match [not] ip6flowlbl label value`
Mode	IPv6-Class-Map Config

match protocol

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. The currently supported values are: **icmp**, **igmp**, **ip**, **tcp**, **udp**. A value of **ip** matches all protocol number values.

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. Use the [not] option to negate the match condition.

Note: This command does not validate the protocol number value against the current list defined by IANA.

Default	none
Format	`match [not] protocol {protocol-name | number}`
Mode	Class-Map Config Ipv6-Class-Map Config

match source-address mac

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). Use the **not** option to negate the match condition.

Default	none
Format	`match [not] source-address mac` *`address macmask`*
Mode	Class-Map Config Ipv6-Class-Map Config

match srcip

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. Use the **`not`** option to negate the match condition.

Default	none
Format	`match [not] srcip` *`ipaddr ipmask`*
Mode	Class-Map Config

match srcip6

This command adds to the specified class definition a match condition based on the source IP address of a packet. Use the **`not`** option to negate the match condition.

Default	none
Format	`match [not] srcip6` *`source-ipv6-prefix/prefix-length`*
Mode	Ipv6-Class-Map Config

match srcl4port

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. Use the **`not`** option to negate the match condition.

Default	none
Format	`match [not] srcl4port {`*`portkey`* `|` *`port-number`*`}`
Mode	Class-Map Config Ipv6-Class-Map Config

match vlan

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. Use the **not** option to negate the match condition.

Default	none
Format	`match [not] vlan` *vland-id*
Mode	Class-Map Config Ipv6-Class-Map Config

match secondary-vlan

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. Use the **not** option to negate the match condition.

Default	none
Format	`match [not] secondary-vlan` *vlan-id*
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/deletion, class addition/removal, and 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`**.

assign-queue

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 device.

Format	`assign-queue` *`queueid`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop

drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

Format	`drop`
Mode	Policy-Class-Map Config
Incompatibilities	Assign Queue, Mark (all forms), Mirror, Police, Redirect

mirror

This command specifies that all incoming packets for the associated traffic stream are copied to a specific egress interface (physical port or LAG).

Format	`mirror` *`unit/slot/port`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Redirect

redirect

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	`redirect` *`unit/slot/port`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mirror

conform-color

Use this command to enable color-aware traffic policing and define the conform-color class map. Used 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: This command may only be used after specifying a police command for the policy-class instance.

Format	`conform-color` *`class-map-name`*
Mode	Policy-Class-Map Config

class

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 is 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	`class` *`classname`*
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	`no class classname`
Mode	Policy-Map Config

mark cos

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	`mark-cos value`
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

mark cos-as-sec-cos

This command marks outer VLAN tag priority bits of all packets as the inner VLAN tag priority, marking Cos as Secondary CoS. This essentially means that the inner VLAN tag CoS is copied to the outer VLAN tag CoS.

Format	`mark cos-as-sec-cos`
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

Command example:

```
(NETGEAR Switch) (Config-policy-classmap)#mark cos-as-sec-cos
```

mark ip-dscp

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	`mark ip-dscp` *dscpval*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police

mark ip-precedence

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	`mark ip-precedence` *value*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police
Policy Type	In

police-simple

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) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128.

For each outcome, the only possible actions are drop, set-cos-as-sec-cos, set-cos-transmit, set-sec-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 once the style is configured.

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.

For **set-cos-transmit** an 802.1p priority value is required and is specified as an integer from 0-7.

Format	police-simple {*1-4294967295 1-128* conform-action {drop | set-cos-as-sec-cos | set-cos-transmit *0-7* | set-sec-cos-transmit *0-7* | set-prec-transmit *0-7* | set-dscp-transmit *0-63* | transmit} [violate-action {drop | set-cos-as-sec-cos | set-cos-transmit *0-7* | set-sec-cos-transmit *0-7* | set-prec-transmit *0-7* | set-dscp-transmit *0-63* | transmit}]}
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

This command is the single-rate form of the **police** command and is used to establish the traffic policing style for the specified class. For each outcome, the only possible actions are drop, set-cos-as-sec-cost, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this single-rate form of the **police** command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

Format	police-single-rate {*1-4294967295 1-128 1-128* conform-action {drop | set-cos-as-sec-cos | set-cos-transmit *0-7* | set-sec-cos-transmit *0-7* | set-prec-transmit *0-7* | set-dscp-transmit *0-63* | transmit} exceed-action {drop | set-cos-as-sec-cos | set-cos-transmit *0-7* | set-sec-cos-transmit *0-7* | set-prec-transmit *0-7* | set-dscp-transmit *0-63* | transmit} [violate-action {drop | set-cos-as-sec-cos-transmit | set-cos-transmit *0-7* | set-sec-cos-transmit *0-7* | set-prec-transmit *0-7* | set-dscp-transmit *0-63* | transmit}]}
Mode	Policy-Class-Map Config

police-two-rate

This command is the two-rate form of the **police** command and is used to establish the traffic policing style for the specified class. For each outcome, the only possible actions are drop, set-cos-as-sec-cos, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this two-rate form of the **police** command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

Format	police-two-rate {*1-4294967295 1-4294967295 1-128 1-128* conform-action {drop | set-cos-as-sec-cos | set-cos-transmit *0-7* | set-sec-cos-transmit *0-7* | set-prec-transmit *0-7* | set-dscp-transmit *0-63* | transmit} exceed-action {drop | set-cos-as-sec-cos | set-cos-transmit *0-7* | set-sec-cos-transmit *0-7* | set-prec-transmit *0-7* | set-dscp-transmit *0-63* | transmit} [violate-action {drop | set-cos-as-sec-cos | set-cos-transmit *0-7* | set-sec-cos-transmit *0-7* | set-prec-transmit *0-7* | set-dscp-transmit *0-63* | transmit}]}
Mode	Policy-Class-Map Config

policy-map

This command establishes a new DiffServ policy. The *policyname* 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	policy-map *policyname* {in | out}
Mode	Global Config

no policy-map

This command eliminates an existing DiffServ policy. The *policyname* parameter is the name of an existing DiffServ policy. This command may be issued at any time. If the policy is currently referenced by one or more interface service attachments, this delete attempt fails.

Format	no policy-map *policyname*
Mode	Global Config

policy-map rename

This command changes the name of a DiffServ policy. The *policyname* is the name of an existing DiffServ class. The *newpolicyname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy.

Format	policy-map rename *policyname newpolicyname*
Mode	Global 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

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 *policyname* parameter is 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	service-policy {in | out} *policymapname*
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 *policyname* 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	`no service-policy {in | out} policymapname`
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

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 class-name`
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.)
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

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. This command takes no options.

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

This command displays all configuration information for the specified policy. The *policyname* is the name of an existing DiffServ policy.

Format	`show policy-map [`*`policyname`*`]`
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 Routing) #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 Routing) #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

This command displays policy service information for the specified interface and direction. The *unit/slot/port* parameter specifies a valid *unit/slot/port* number for the system.

Format	`show diffserv service` *unit/slot/port* `in`
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	*unit/slot/port*
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.
Policy Details	Attached policy details, whose content is identical to that described for the show policy-map *policymapname* command (content not repeated here for brevity).

show diffserv service brief

This command displays all interfaces in the system to which a DiffServ policy has been attached. The inbound direction parameter is optional.

Format	`show diffserv service brief [in]`
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	*unit/slot/port*
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

This command displays policy-oriented statistics information for the specified interface and direction. The *unit/slot/port* parameter specifies a valid interface for the system. 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.

Note: This command is only allowed while the DiffServ administrative mode is enabled.

Format	`show policy-map interface` *unit/slot/port* `[in]`
Mode	Privileged EXEC

Term	Definition
Interface	*unit/slot/port*
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

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction.

Format	`show service-policy in`
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	*unit/slot/port*
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

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 is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list. The rate-limit attribute configures the committed rate and the committed burst size.

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` *name*
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` *name*
Mode	Global Config

mac access-list extended rename

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` *name newname*
Mode	Global Config

{deny | permit} (MAC ACL)

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	{deny | permit} {*srcmac* | any} {*dstmac* | any} [*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: The **no** form of this command is not supported, since the rules within a MAC ACL cannot be deleted individually. Rather, the entire MAC ACL must be deleted and respecified.

Note: An implicit **deny all** MAC rule always terminates the access list.

The Ethertype may be specified 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 15. 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 1094.

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. 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 *unit/slot/port*, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified *unit/slot/port*. The **assign-queue** and **redirect** parameters are only valid for a **permit** rule.

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, and *burst-size* in kbytes.

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
```

mac access-group

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 given 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 keyword **control-plane** is only available in Global Config mode.

Note: You should be aware that the **out** option may or may not be available, depending on the platform.

Format	`mac access-group` *`name`* `{{control-plane | in | out} vlan` *`vlan-id`* `{in | out}} [sequence` *`1-4294967295`*`]`
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 in a given direction.
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.

Command example:

```
(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 given direction.

Format	`no mac access-group` *`name`* `{{control-plane | in | out} vlan` *`vlan-id`* `{in | out}}`
Modes	Global Config Interface Config

Command example:

```
(NETGEAR Switch)(Config)#no mac access-group mac1 control-plane
```

show mac access-lists

This command displays a MAC access list and all of the rules that are defined for the MAC ACL. Use the optional *name* parameter to identify a specific MAC ACL to display.

Note: The command output varies based on the match criteria configured within the rules of an ACL.

Format	`show mac access-lists [name]`
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.
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 unit/slot/port to which packets matching this rule are copied.
Redirect Interface	The *unit/slot/port* 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.

Command example:

```
(NETGEAR Routing) #show mac access-lists mac1

ACL Name: mac1

Outbound Interface(s): control-plane

Rule Number: 1
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
```

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

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. *Table 16* on page 1074 describes the parameters for the **`access-list`** command.

IP Standard ACL:

Format	`access-list` *`1-99`* `{deny | permit} {every | srcip srcmask} [log] [time-range` *`time-range-name`*`] [assign-queue` *`queue-id`*`] [{mirror | redirect}` *`unit/slot/port`*`]`
Mode	Global Config

IP Extended ACL:

Format	access-list *100-199* {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*]}} [time-range *time-range-name*] [log] [assign-queue *queue-id*] [{mirror | redirect} *unit/slot/port*] [rate-limit *rate burst-size*]
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.

Table 16. ACL command parameters

Parameter	Description
1-99 or *100-199*	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.
{deny | permit}	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.
every	Match every packet.
{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | *0-255*}	Specifies the protocol to filter for an extended IP ACL rule.
srcip srcmask | any | host *scrip*	Specifies a source IP address and source netmask for match condition of the IP ACL rule. Specifying any specifies *srcip* as 0.0.0.0 and *srcmask* as 255.255.255.255. Specifying host *A.B.C.D* specifies *srcip* as A.B.C.D and *srcmask* as 0.0.0.0.

Table 16. ACL command parameters (continued)

Parameter	Description
[{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}]	**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 *portkey*, 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 *startport* and *endport* 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.
dstip dstmask |any | host *dstip*	Specifies a destination IP address and netmask for match condition of the IP ACL rule. Specifying any implies specifying *dstip* as 0.0.0.0 and *dstmask* as 255.255.255.255. Specifying host A.B.C.D implies *dstip* as A.B.C.D and *dstmask* as 0.0.0.0.
[precedence *precedence* | tos *tos* [*tosmask*] | dscp *dscp*]	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters *precedence*, *tos* or *dscp*. *tosmask* is an optional parameter.

Table 16. ACL command parameters (continued)

Parameter	Description
`flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]`	**Note:** This option is available only if the protocol is tcp. Specifies that the IP ACL rule matches on the TCP flags. When +<tcpflagname> is specified, a match occurs if the specified <tcpflagname> flag is set in the TCP header. When -<tcpflagname> is specified, a match occurs if the specified <tcpflagname> flag is not set in the TCP header. When established 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 established option is specified.
`[icmp-type` *`icmp-type`* `[icmp-code` *`icmp-code`*`] | icmp-message` *`icmp-message`*`]`	**Note:** This option is available only if the protocol is **`icmp`**. Specifies a match condition for ICMP packets. When **`icmp-type`** is specified, the IP ACL rule matches on the specified ICMP message type, a number from 0 to 255. When **`icmp-code`** is specified, the IP ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying **`icmp-message`** implies that both *`icmp-type`* and *`icmp-code`* are specified. The following *`icmp-message`* 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`**.
`igmp-type` *`igmp-type`*	This option is available 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.
`fragments`	Specifies that the IP ACL rule matches on fragmented IP packets.
`[log]`	Specifies that this rule is to be logged.
`[time-range` *`time-range-name`*`]`	Allows imposing time limitation on the ACL rule as defined by the parameter *`time-range-name`*. 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 1094.
`[assign-queue` *`queue-id`*`]`	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
`[{mirror | redirect}` *`unit/slot/port`*`]`	Specifies the mirror or redirect interface which is the *`unit/slot/port`* to which packets matching this rule are copied or forwarded, respectively.
`[rate-limit` *`rate burst-size`*`]`	Specifies the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

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	`no access-list` *accesslistnumber*
Mode	Global Config

ip access-list

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	`ip access-list` *name*
Mode	Global Config

no ip access-list

This command deletes the IP ACL identified by name from the system.

Format	`no ip access-list` *name*
Mode	Global Config

ip access-list rename

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 is an IP ACL by the name that is defined by *newname* already exists.

Format	`ip access-list rename` *name newname*
Mode	Global Config

{deny | permit} (IP ACL)

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	{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*]}} [time-range *time-range-name*] [log] [assign-queue *queue-id*] [{mirror | redirect} *unit/slot/port*] [rate-limit *rate burst-size*]
Mode	Ipv4-Access-List Config

Note: The **no** form of this command is not supported, since the rules within an IP ACL cannot be deleted individually. Rather, the entire IP ACL must be deleted and respecified.

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 *unit/slot/port*, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified *unit/slot/port*. 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 1094.

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. 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.

Table 17. IP ACL command parameters

Parameter	Description
{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.
srcip *srcmask* | any | host *srcip*	Specifies a source IP address and source netmask to match for the IP ACL rule. Specifying "any" implies specifying *srcip* as "0.0.0.0" and *srcmask* as "255.255.255.255". Specifying "host A.B.C.D" implies *srcip* as "A.B.C.D" and *srcmask* as "0.0.0.0".

Table 17. IP ACL command parameters (continued)

Parameter	Description
[{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}]	**Note:** This option is available only if the protocol is **tcp** or **udp**. 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: **bgp**, **domain**, **echo**, **ftp**, **ftp-data**, **http**, **smtp**, **telnet**, **www**, **pop2**, or **pop3**. For udp protocol: **domain**, **echo**, **ntp**, **rip**, **snmp**, **tftp**, **time**, or **who**. 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 *startport* and *endport* 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.
dstip dstmask | any | host *dstip*	Specifies a destination IP address and netmask for match condition of the IP ACL rule. Specifying any implies specifying *dstip* as 0.0.0.0 and *dstmask* as 255.255.255.255. Specifying host A.B.C.D implies *dstip* as A.B.C.D and *dstmask* as 0.0.0.0.
[precedence *precedence* | tos *tos* [*tosmask*] | dscp *dscp*]	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters *precedence*, *tos* or *dscp*. *tosmask* is an optional parameter.

Table 17. IP ACL command parameters (continued)

Parameter	Description
`flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]`	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.
`[icmp-type` *`icmp-type`* `[icmp-code` *`icmp-code`*`] | icmp-message` *`icmp-message`*`]`	**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 *`icmp-type`* and *`icmp-code`* are specified. The following *`icmp-message`* 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.
`igmp-type` *`igmp-type`*	**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.
`fragments`	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.
`log`	Specifies that this rule is to be logged.
`time-range` *`time-range-name`*	Allows imposing a time limitation on the ACL rule as defined by the parameter *`time-range-name`*. 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.
`assign-queue` *`queue-id`*	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.

Table 17. IP ACL command parameters (continued)

Parameter	Description
{mirror | redirect} *unit/slot/ port*	Specifies the mirror or redirect interface which is the *unit/slot/port* to which packets matching this rule are copied or forwarded, respectively.
rate-limit *rate burst-size*	Specifies the allowed rate of traffic as per the configured *rate* in kbps, and *burst-size* in kbytes.

Command example:

```
(NETGEAR Routing) (Config)#ip access-list ip1

(NETGEAR Routing) (Config-ipv4-acl)#permit icmp any any rate-limit 32 16

(NETGEAR Routing) (Config-ipv4-acl)#exit
```

ip access-group

This command either attaches a specific IP Access Control List (ACL) identified by *accesslistnumber* or *name* to an interface, range of interfaces, or all interfaces; or associates it with a VLAN ID in a given 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 keyword **control-plane** is only available in Global Config mode.

Note: You should be aware that the **out** option may or may not be available, depending on the platform.

Default	none
Format	`ip access-group {`*`accesslistnumber`* `|` *`name`*`} {{control-plane| in	out}	vlan` *`vlan-id`* `{in	out}} [sequence` *`1-4294967295`*`]`
Modes	Interface Config Global Config

Parameter	Description
accesslistnumber	Identifies a specific IP ACL. The range is 1 to 199.
name	The name of the Access Control List.
vlan-id	A VLAN ID associated with a specific IP ACL in a given direction.
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.

Command example:

```
(NETGEAR Switch) (Config)#ip access-group ip1 control-plane
```

no ip access-group

This command removes a specified IP ACL from an interface.

Default	none
Format	`no ip access-group {`*`accesslistnumber`* `|` *`name`*`} {{control-plane	in	out}| vlan` *`vlan-id`* `{in	out}}`
Mode	Interface Config Global Config

Command example:

```
(NETGEAR Switch)(Config)#no ip access-group ip1 control-plane
```

acl-trapflags

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

Use this command to view summary information about all IP ACLs 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.

Format	`show ip access-lists [`*`accesslistnumber`* `|` *`name`*`]`
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.

Term	Definition
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.
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/slot/port to which packets matching this rule are copied.
Redirect Interface	The unit/slot/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.

Command example:

```
(NETGEAR Routing) #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
```

show access-lists

This command displays IP ACLs, IPv6 ACLs, and MAC access control lists information for a designated interface and direction. The *unit/slot/port* parameter specifies a valid interface for the system. 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 **control-plane** keyword to display the ACLs applied on the CPU port.

Format	show access-lists interface {*unit/slot/port* {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

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 *vlan-id* [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

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	`ipv6 access-list` *name*
Mode	Global Config

no ipv6 access-list

This command deletes the IPv6 ACL identified by *name* from the system.

Format	`no ipv6 access-list` *name*
Mode	Global Config

ipv6 access-list rename

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 is an IPv6 ACL by the name that is specified by the *newname* argument already exists.

Format	`ipv6 access-list rename` *name newname*
Mode	Global Config

{deny | permit} (IPv6)

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	`{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*`] [routing] [fragments] [dscp` *dscp*`]}} [log] [assign-queue` *queue-id*`] [{mirror | redirect}` *unit/slot/port*`] [rate-limit` *rate burst-size*`]`
Mode	IPv6-Access-List Config

Note: The **no** form of this command is not supported, since the rules within an IPv6 ACL cannot be deleted individually. Rather, the entire IPv6 ACL must be deleted and respecified.

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 1094.

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. 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 *unit/slot/port*, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified *unit/slot/port*. 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.

Table 18. 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.**
source-ipv6-prefix/prefix-length | any | *host source-ipv6-address*	For *source-ipv6-prefix/prefix-length*, specify a source IPv6 source address and prefix length to match for the IPv6 ACL rule. Specifying **any** implies specifying ::/0 Specifying *host source-ipv6-address* implies matching the specified IPv6 address. The *source-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Table 18. IPv6 ACL command parameters (continued)

Parameter	Description
[eq {*portkey* | *0-65535*}]	**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 *portkey*, 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>
destination-ipv6-prefix/prefix-length | any | *host destination-ipv6-address*	For *destination-ipv6-prefix/prefix-length*, specify a destination IPv6 source address and prefix length to match for the IPv6 ACL rule. Specifying **any** implies specifying ::/0 Specifying *host destination-ipv6-address* implies matching the specified IPv6 address. This *destination-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
[dscp *dscp*]	Specifies the *dscp* value to match for the IPv6 rule.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	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 established 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 18. IPv6 ACL command parameters (continued)

Parameter	Description
[icmp-type *icmp-type* [icmp-code *icmp-code*] | icmp-message *icmp-message*]	**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 *icmp-type* and *icmp-code* are specified. The following *icmp-message* 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.
fragments	Specifies that IPv6 ACL rule matches on fragmented IPv6 packets (Packets that have the next header field is set to 44).
routing	Specifies that IPv6 ACL rule matches on IPv6 packets that have routing extension headers (the next header field is set to 43).
log	Specifies that this rule is to be logged.
time-range *time-range-name*	Allows imposing a time limitation on the ACL rule as defined by the parameter *time-range-name*. 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.
assign-queue *queue-id*	Specifies the assign-queue, which is the queue identifier (*queue-id*) to which packets matching this rule are assigned.
{mirror | redirect} *unit/slot/port*	Specifies the mirror or redirect interface which is the unit/slot/port to which packets matching this rule are copied or forwarded, respectively.
rate-limit *rate burst-size*	Specifies the allowed rate of traffic as per the configured *rate* in kbps, and *burst-size* in kbytes.

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
```

ipv6 traffic-filter

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 given 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 keyword **control-plane** is only available in Global Config mode.

Note: You should be aware that the **out** option may or may not be available, depending on the platform.

Format	`ipv6 traffic-filter` *`name`* `{{control-plane |in | out} |vlan` *`vlan-id`* `{in | out}} [sequence` *`1-4294967295`*`]`
Modes	Global Config Interface Config

Command example:

```
(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 given direction.

Format	`no ipv6 traffic-filter` **`name`** `{{control-plane | in | out} | vlan` *`vlan-id`* `{in | out}}`
Modes	Global Config Interface Config

Command example:

```
(NETGEAR Switch) (Config)#no ipv6 traffic-filter ip61 control-plane
```

show ipv6 access-lists

This command displays an IPv6 access list and all of the rules that are defined for the IPv6 ACL. Use the optional *name* parameter to identify a specific IPv6 ACL to display.

Format	`show ipv6 access-lists [`*`name`*`]`
Mode	Privileged EXEC

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 ordered rule number identifier defined within the IPv6 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.
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.

Term	Definition
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 *unit/slot/port* to which packets matching this rule are copied.
Redirect Interface	The *unit/slot/port* 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.
Rule Status	Status (Active/Inactive) of the IPv6 ACL rule.

Command example:

```
(NETGEAR Routing) #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
```

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

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` *`name`*
Mode	Global Config

no time-range

This command deletes a time-range identified by *name*.

Format	`no time-range` *`name`*
Mode	Global Config

absolute

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` *`time date`*`] [end` *`time date`*`]`
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

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 *days-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	`periodic` *`days-of-the-week time`* `to` *`time`*
Mode	Time-Range Config

no periodic

This command deletes a periodic time entry from a time range.

Format	`no periodic` *`days-of-the-week time`* `to` *`time`*
Mode	Time-Range Config

show time-range

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	`show time-range [`*`name`*`]`
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.
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

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.

auto-voip oui

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 *`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` *`oui-prefix`* `desc` *`string`*
Mode	Global Config

Command example:

The following example adds an OUI to the table:

```
(NETGEAR Switch) (Config)#auto-voip oui 00:03:6B desc "Cisco 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` *`oui-prefix`*
Mode	Global Config

auto-voip oui-based priority

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	`auto-voip oui-based priority` *`priority-value`*
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	`no auto-voip oui-based priority`
Mode	Global Config Interface Config

auto-voip protocol-based

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 to ensure voice traffic always gets the highest priority throughout the network path.

The *`tc`* value is the traffic class used for protocol-based VoIP traffic. 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` *`remark-priority`* `| traffic-class` *`tc`*`}`
Mode	Global Config Interface 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` *`remark-priority`* `| traffic-class` *`tc`*`}`
Mode	Global Config Interface Config

auto-voip vlan

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` *`vlan-id`*
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

Use this command to display the auto VoIP settings on one particular interface or on all interfaces of the switch.

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.

Field	Description
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     Operational Status
                  Mode
---------    -------------- -----------------
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

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

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

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	`iscsi aging time` *`time`*
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

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 chassis 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 enable

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 will be released.

Format	no iscsi enable
Mode	Global Config

iscsi target port

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` *`tcp-port-1`* `[`*`tcp-port-2...tcp-port-16`*`] [address` *`ip-address`*`] [name` *`targetname`*`]`
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

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

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
```

IP Multicast Commands

15

This chapter describes the IP multicast commands available in the NETGEAR Managed Switch CLI. The chapter contains the following sections:

- *Multicast Commands*
- *DVMRP Commands*
- *PIM Commands*
- *Internet Group Message Protocol Commands*
- *IGMP Proxy Commands*

Only the following switches support IP mulicast:

- M6100
- M5300-28G3
- M5300-52G3
- M5300-28GF3

The following switches support IP muliticast with an L3 license:

- M5300-28G
- M5300-52G
- M5300-28G-POE+
- M5300-52G-POE+

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

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	`ip mcast boundary` *groupipaddr mask*
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	`no ip mcast boundary` *groupipaddr mask*
Mode	Interface Config

ip mroute

This command configures an IPv4 multicast static route for a source.

Default	No MRoute is configured on the system.
Format	`ip mroute` *src-ip-addr src-mask rpf-addr preference*
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.
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	`no ip mroute` *`src-ip-addr`*
Mode	Global Config

ip multicast

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

This command is specific to IPv4. Use this command to apply the given Time-to-Live threshold value to a routing interface or range of interfaces. The *`ttlvalue`* is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface. This command sets the Time-to-Live threshold value such that any data packets forwarded over the interface having TTL value above the configured value are dropped. The value for *`ttlvalue`* ranges from 0 to 255.

Default	1
Format	`ip multicast ttl-threshold` *`ttlvalue`*
Mode	Interface Config

no ip multicast ttl-threshold

This command applies the default TTL threshold to a routing interface. The TTL threshold is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface.

Format	`no ip multicast ttl-threshold`
Mode	Interface Config

show ip mcast

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

This command displays all the configured administrative scoped multicast boundaries.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the unit/slot/port format. The *vlan-id* parameter is a number in the range of 1–4093.

Format	`show ip mcast boundary {`*unit/slot/port* `| vlan` *vlan-id* `| all}`
Modes	Privileged EXEC User EXEC

Term	Definition
Interface	*unit/slot/port*

Term	Definition
Group Ip	The group IP address.
Mask	The group IP mask.

show ip mcast interface

This command displays the multicast information for the specified interface.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the unit/slot/port format. The *vlan-id* parameter is a number in the range of 1–4093.

Format	`show ip mcast interface {`*`unit/slot/port`* `| vlan` *`vlan-id`*`}`
Modes	Privileged EXEC User EXEC

Term	Definition
Interface	*unit/slot/port*
TTL	The time-to-live value for this interface.

show ip mcast mroute

This command displays a summary or all the details of the multicast table.

Format	`show ip mcast 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 mcast mroute group

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 mroute table containing the given *groupipaddr*.

Format	`show ip mcast mroute group` *groupipaddr* `{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 ip mcast mroute source

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 mroute table containing the given source IP address (*sourceipaddr*) or source IP address and group IP address (*groupipaddr*) pair.

Format	`show ip mcast mroute source` *sourceipaddr* `{summary |` *groupipaddr*`}`
Modes	Privileged EXEC User EXEC

If you use the *groupipaddr* 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.
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 mcast mroute static

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 mcast mroute static [sourceipaddr]`
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 mcast 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
```

clear ip mroute

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	`clear ip mroute {* | group-address [source-address]}`
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 Routing) # 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 Routing) # 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 Routing) # clear ip mroute 224.1.2.1 192.168.10.10
```

DVMRP Commands

This section describes the Distance Vector Multicast Routing Protocol (DVMRP) commands.

ip dvmrp (Global Config)

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

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 1 to 31.

Default	1
Format	`ip dvmrp metric` *`metric`*
Mode	Interface Config

no ip dvmrp metric

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

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)

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

This command sets the administrative mode of DVMRP on an interface to inactive.

Format	`no ip dvmrp`
Mode	Interface Config

show ip dvmrp

This command displays the system-wide information for DVMRP.

Format	`show ip dvmrp`
Modes	Privileged EXEC User EXEC

Term	Definition
Admin Mode	Indicates whether DVMRP is enabled or disabled.
Version String	The version of DVMRP being used.

Term	Definition
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	*unit/slot/port*
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

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 *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the unit/slot/port format. The *vlan-id* parameter is a number in the range of 1–4093.

Format	show ip dvmrp interface {*unit/slot/port* | vlan *vland-id*}
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.

Term	Definition
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

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

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 *unit/slot/port* format for the outgoing interface for this next hop.
Type	The network is a LEAF or a BRANCH.

show ip dvmrp prune

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

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

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

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

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

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` *seconds*
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

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 in 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-candidate

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR).

The argument *`unit/slot/port`* corresponds to a physical routing interface or VLAN routing interface. The **`vlan`** keyword and *`vland-id`* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the unit/slot/port format. 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 {`*`unit/slot/port`* `| vlan` *`vlan-id`*`}` *`hash-mask-length`* `[`*`bsr-priority`*`] [interval` *`interval`*`]`
Mode	Global Config

Parameters	Description
unit/slot/port	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.
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

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` *`priority`*
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

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` *`seconds`*
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

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	`ip pim rp-address` *`rp-address group-address group-mask`* `[override]`
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.
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	`no ip pim rp-address` *`rp-address group-address group-mask`* `[override]`
Mode	Global Config

ip pim rp-candidate

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 argument *`unit/slot/port`* corresponds to a physical routing interface or VLAN routing interface. The **`vlan`** keyword and *`vland-id`* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the unit/slot/port format. 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 rp-candidate interface {`*`unit/slot/port`* `| vlan` *`vland-id`*`} group-address group-mask [interval` *`interval`*`]`
Mode	Global Config

Parameter	Description
unit/slot/port or vland-id	The interface type in the *`unit/slot/port`* format 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.

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) for a specific multicast group range.

Format	`no ip pim rp-candidate interface {`*`unit/slot/port`* `| vlan` *`vland-id`*`} group-address group-mask`
Mode	Global Config

ip pim ssm

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 {default | group-address group-mask}`
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 {default | group-address group-mask}`
Mode	Global Config

ip pim-trapflags

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 pim

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	*unit/slot/port*
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.

Command example:

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

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

This command displays the PIM interface status parameters.

The argument *`unit/slot/port`* corresponds to a physical routing interface or VLAN routing interface. The **`vlan`** keyword and *`vland-id`* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the unit/slot/port format. 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.

Format	`show ip pim interface [`*`unit/slot/port`* `| vlan` *`vlan-id`*`]`
Modes	Privileged EXEC User EXEC

Term	Definition
Interface	*`unit/slot/port`*, which is 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

This command displays PIM neighbors discovered by PIMv2 Hello messages.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the unit/slot/port format. 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	`show ip pim neighbor [`*`unit/slot/port`* `| vlan` *`vlan-id`*`]`
Modes	Privileged EXEC User EXEC

Term	Definition
Neighbor Address	The IP address of the PIM neighbor on an interface.
Interface	*unit/slot/port*
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      Expiry Time DR
                           (hh:mm:ss) (hh:mm:ss)   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

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

This command displays the rendezvous point (RP) selected for the specified group address.

Format	`show ip pim rp-hash` *`group-address`*
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

Use this command to display the mapping for the PIM group to the active Rendezvous points (RP) of which the router is a 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 [`*rp-address*` | 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.
```

Internet Group Message Protocol Commands

This section describes the commands you use to view and configure Internet Group Message Protocol (IGMP) settings.

ip igmp

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

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

This command configures the version of IGMP for an interface or range of interfaces. The value for *`version`* is either 1, 2 or 3.

Default	3
Format	`ip igmp version` *`version`*
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

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	`ip igmp last-member-query-count` *`count`*
Modes	Interface Config

no ip igmp last-member-query-count

This command resets the number of Group-Specific Queries to the default value.

Format	`no ip igmp last-member-query-count`
Modes	Interface Config

ip igmp last-member-query-interval

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	`ip igmp last-member-query-interval` *deciseconds*
Modes	Interface Config

no ip igmp last-member-query-interval

This command resets the Maximum Response Time to the default value.

Format	`no ip igmp last-member-query-interval`
Modes	Interface Config

ip igmp query-interval

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	`ip igmp query-interval` *seconds*
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	`no ip igmp query-interval`
Modes	Interface Config

ip igmp query-max-response-time

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	`ip igmp query-max-response-time` *`desciseconds`*
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	`no ip igmp query-max-response-time`
Mode	Interface Config

ip igmp robustness

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` *`number`*
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

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` *number*
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

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	`ip igmp startup-query-interval` *seconds*
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	`no ip igmp startup-query-interval`
Mode	Interface Config

show ip igmp

This command displays the system-wide IGMP information.

Format	`show ip igmp`
Modes	Privileged EXEC User EXEC

Term	Definition
IGMP Admin Mode	The administrative status of IGMP. This is a configured value.
Interface	*unit/slot/port*
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

This command displays the registered multicast groups on the interface.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the unit/slot/port format. 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 {*unit/slot/port* | vlan *vland-id*} [detail]
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.

Term	Definition
Up Time	The time elapsed since the entry was created for the specified multicast group address on this interface.
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

This command displays the IGMP information for the interface.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the unit/slot/port format. 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	*unit/slot/port*
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 be have a lot of loss, the Robustness variable may be increased for that interface.
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.

Term	Definition
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

This command displays the list of interfaces that registered in the multicast group. The *multiipaddr* argument specifies the IP address of the multicast group.

Format	`show ip igmp interface membership` *`multiipaddr`* `[detail]`
Mode	Privileged EXEC

Term	Definition
Interface	Valid unit, slot and port number separated by forward slashes.
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, slot and port number separated by forward slashes.
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.
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

This command displays the IGMP statistical information for the interface. The statistics are only displayed when the interface is enabled for IGMP.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the unit/slot/port format. The *vlan-id* parameter is a number in the range of 1–4093.

Format	show ip igmp interface stats [*unit/slot/port* | vlan *vland-id*]
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

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, make sure that there are no multicast routing protocols enabled on the router.

Format	ip igmp-proxy
Mode	Interface Config

no ip igmp-proxy

This command disables the IGMP Proxy on the router.

Format	`no ip igmp-proxy`
Mode	Interface Config

ip igmp-proxy unsolicit-rprt-interval

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	`ip igmp-proxy unsolicit-rprt-interval` *seconds*
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

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

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.
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 Routing) #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

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 *unit/slot/port* 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 Routing) #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

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 Routing) #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

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.

Term	Definition
Sources	The number of sources attached to the multicast group.
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 Routing) #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
```

IPv6 Multicast Commands

16

The entire IPv6 Multicast commands section is Enterprise-only. This chapter describes the IPv6 Multicast commands available in the NETGEAR Managed Switch CLI.

The chapter contains the following sections:

- *IPv6 Multicast Forwarder*
- *IPv6 PIM Commands*
- *IPv6 MLD Commands*
- *IPv6 MLD-Proxy Commands*

Only the following switches support IPv6 multicast:

- M6100
- M5300-28G3
- M5300-52G3
- M5300-28GF3

The following switches support IPv6 multicast with an L3 license:

- M5300-28G
- M5300-52G
- M5300-28G-POE+
- M5300-52G-POE+

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

This command configures an IPv6 Multicast Static Route for a source.

Default	No MRoute is configured on the system.
Format	`ipv6 mroute` *`src-ip-addr src-mask rpf-addr`* [*`interface`*] *`preference`*
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.
rpf-ip-addr	The IP address of the RPF next-hop router toward the source.
interface	[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	`no ip mroute` *`src-ip-addr`*
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

Use this command to show the mroute entries that are specific to IPv6. (This command is the IPv6 equivalent of the IPv4 **`show ip mcast mroute`** command.)

Format	`show ipv6 mroute [[detail] | [summary] | [group {`*`group-address`*`} [detail | summary]] | [source {`*`source-address`*`} [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

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 mroute table containing the given group IPv6 address *group-address*.

Format	`show ipv6 mroute group` *`group-address`* `{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

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 mroute table containing the given source IP address (*source-address*) or source IP address and group IP address (*groupipaddr*) pair.

Format	`show ipv6 mroute source` *source-address* {*groupipaddr* | summary}
Modes	Privileged EXEC User EXEC

If you use the *groupipaddr* 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.
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 ipv6 mroute static

Use the **show ipv6 mroute static** command in Privileged EXEC or User EXEC mode to display all the configured IPv6 multicast static routes.

Format	`show ipv6 mroute static [`*source-address*`]`
Modes	Privileged EXEC User EXEC

Parameter	Description
Source Address	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.
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

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	`clear ipv6 mroute {* | group-address [source-address]}`
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.

Command example:

The following example deletes all entries from the IPv6 multicast routing table:

```
(NETGEAR Routing) # 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 Routing) # 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 Routing) # 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

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

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

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

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	`ipv6 pim hello-interval` *seconds*
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	`no ipv6 pim hello-interval`
Mode	Interface Config

ipv6 pim bsr-border

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	`ipv6 pim bsr-border`
Mode	Interface Config

Command example:

```
(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	`no ipv6 pim bsr-border`
Mode	Interface Config

ipv6 pim bsr-candidate

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR).

The argument *`unit/slot/port`* corresponds to a physical routing interface or VLAN routing interface. The **`vlan`** keyword and *`vland-id`* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the unit/slot/port format. 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 bsr-candidate interface {`*`unit/slot/port`* `| vlan` *`vland-id`*`}` *`hash-mask-length`* `[`*`bsr-priority`*`] [interval` *`interval`*`]`
Mode	Global Config

Parameters	Description
unit/slot/port	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 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 {`*`unit/slot/port`* `| vlan` *`vland-id`*`}`
Mode	Global Config

ipv6 pim dr-priority

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` *priority*
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

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	`ipv6 pim join-prune-interval` *seconds*
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	`no ipv6 pim join-prune-interval`
Mode	Interface Config

ipv6 pim rp-address

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	`ipv6 pim rp-address` *`rp-address group-address/prefix-length`* `[override]`
Mode	Global Config

Parameter	Description
rp-address	The IPv6 address of the RP.
group-address/ prefix-length	The group address and prefix length supported by 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` *`rp-address group-address/prefix-length`* `[override]`
Mode	Global Config

ipv6 pim rp-candidate

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 argument *`unit/slot/port`* corresponds to a physical routing interface or VLAN routing interface. The **`vlan`** keyword and *`vland-id`* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the unit/slot/port format. 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 {`*`unit/slot/port`* `| vlan` *`vland-id`*`} group-address group-mask [interval` *`interval`*`]`
Mode	Global Config

Parameter	Description
unit/slot/port or vland-id	The interface type in the *`unit/slot/port`* format 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.

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 group-mask`
Mode	Global Config

ipv6 pim ssm

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 group-mask`*`}`
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 | group-address group-mask}`
Mode	Global Config

show ipv6 pim

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	*unit/slot/port*
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.

Command example:

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

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

This command displays the interface information for PIM on the specified interface.

The argument *`unit/slot/port`* corresponds to a physical routing interface or VLAN routing interface. The **`vlan`** keyword and *`vland-id`* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the unit/slot/port format. 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 [`*`unit/slot/port`* `| vlan` *`vland-id`*`]`
Modes	Privileged EXEC User EXEC

Term	Definition
Interface	*`unit/slot/port`*
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

This command displays PIM neighbors discovered by PIMv2 Hello messages.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the unit/slot/port format. 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.

Format	`show ipv6 pim neighbor [{`*unit/slot/port* `| vlan` *vland-id*`]`
Modes	Privileged EXEC User EXEC

Term	Definition
Neighbor Address	The IPv6 address of the PIM neighbor on an interface.
Interface	*unit/slot/port*
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       Expiry Time
                               (HH:MM::SS)  (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

This command displays the bootstrap router (BSR) information.

Format	`show ipv6 pim bsr-router {candidate | elected}`
Mode	Privileged EXEC User EXEC

Term	Definition
BSR Address	IPv6 address of the BSR.
BSR Priority	Priority as configured in the **`ipv6 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 **`ipv6 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 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

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` *group-address*
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

Use this command to display the mapping for the PIM group to the active Rendezvous points (RP) of which the router is a 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 [`*rp-address* `| 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.

Term	Definition
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.
```

IPv6 MLD Commands

IGMP/MLD Snooping is Layer 2 functionality but IGMP/MLD are Layer 3 multicast protocols. It requires that in a network setup there should be a multicast router (which can act as a querier) to be present to solicit the multicast group registrations. However some network setup does not need a multicast router as multicast traffic is destined to hosts within the same network. In this situation, NETGEAR Managed Switch has an IGMP/MLD Snooping Querier running on one of the switches and Snooping enabled on all the switches. For more information, see *IGMP Snooping Configuration Commands* on page 549 and *MLD Snooping Commands* on page 563.

ipv6 mld router

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

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` *seconds*
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

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` *`milliseconds`*
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 last-member-query-interval

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	`ipv6 mld last-member-query-interval` *`milliseconds`*
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	`no ipv6 mld last-member-query-interval`
Mode	Interface Config

ipv6 mld last-member-query-count

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` *number*
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

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

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 argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the unit/slot/port format. The *vlan-id* parameter is a number in the range of 1–4093. You can also specify a group address (*group-address*).

Format	`show ipv6 mld groups {`*`unit/slot/port`* `| vlan` *`vland-id | group-address`*`}`
Mode	Privileged EXEC User EXEC

The following fields are displayed as a table when *`unit/slot/port`* is specified.

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.
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 Routing) #show ipv6 mld groups ?

group-address            Enter Group Address Info.
<unit/slot/port>         Enter interface in unit/slot/port format.
```

Command example:

```
(NETGEAR Routing) #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 Routing) #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

Use this command to display MLD-related information for the interface.

The argument *unit/slot/port* corresponds to a physical routing interface or VLAN routing interface. The **vlan** keyword and *vland-id* parameter are used to specify the VLAN ID of the routing VLAN directly instead of in the unit/slot/port format. The *vlan-id* parameter is a number in the range of 1–4093.

Format	show ipv6 mld interface {*unit/slot/port* | vlan *vland-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 in *unit/slot/port* format.
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 valued 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

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

Use this command to reset the MLD counters to zero on the specified interface.

Format	`clear ipv6 mld counters` *`unit/slot/port`*
Mode	Privileged Exec

clear ipv6 mld traffic

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

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	`ipv6 mld-proxy`
Mode	Interface Config

no ipv6 mld-proxy

Use this command to disable MLD-Proxy on the router.

Format	`no ipv6 mld-proxy`
Mode	Interface Config

ipv6 mld-proxy unsolicit-rprt-interval

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	`ipv6 mld-proxy unsolicit-rprt-interval` *`interval`*
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	`no ipv6 mld-proxy unsolicit-rprt-interval`
Mode	Interface Config

ipv6 mld-proxy reset-status

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

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 Routing) #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

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 *`unit/slot/port`* of 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 Routing) #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

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 Routing) #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

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.

Field	Description
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 Routing) #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

Group Source List             Expiry Time
------------------            ---------------
3001::1                       00:03:32
3002::2                       00:03:32

FF1E::3          FE80::100:2.3    328        DELAY_MEMBER      Exclude        0
FF1E::4          FE80::100:2.3    255        DELAY_MEMBER      Include        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
```

17 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 NETGEAR Managed Switch software supports PoE, PoE+, and UPoE as follows:

- **PoE (802.3af 2003)**. 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-2009)**. This is a newer standard than PoE. This 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.
- **UPoE**. Universal Power over Ethernet (UPoE) extends PoE+ to deliver up to 60W. For a 48-port switch, UPoE can provide a total of 2,880 watts power budget for all ports. UPoE delivers the power over a spare pair or Alternate B pair (4,5 and 7,8) simultaneously along with the data pair or Alternate A pair (1,2 and 3,6). Power beyond 30 watts is always delivered using the data and spare pair. UPoE provides two options for enabling the spare pair: LLDP, which is the preferred method, and forced UPoE. UPoE also supports green modes of operation.

  Note: UPoE is supported on the M6100 series switches only.

Note: PoE, PoE+, and UPoE are supported only on physical, copper interfaces. The default port mode is PoE+.

PoE Commands

poe

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

Use this command to configure the detection type on a global basis or per interface. It is used to configure which types of PDs will be detected and powered by the switch. There are three options:

- **ieee**—Detect resistive-type devices (IEEE standard)
- **pre-ieee**—Legacy capacitive detection only (nonstandard)
- **auto**—Perform resistive detection first (IEEE standard) and capacitive detection (pre-IEEE standard)

Default	auto
Format	poe detection {ieee | pre-ieee | auto}
Mode	Global Config Interface Config

no poe detection

Use this command to set the detection mode to the default on a global basis or per interface.

Format	no poe detection
Mode	Global Config Interface Config

poe high-power

Use this command to switch a port from 802.3af mode to high-power mode. This mode is used to power up devices that require more power than the current IEEE 802.3af power (more than 12.95 watts at the PD). There are three options:

- **legacy**–Use this mode if the device can power up (more than 12.95 watts) with higher current and it cannot identify itself as a Class 4 device.
- **pre-dot3at**–Use this mode if the device cannot identify itself as a Class 4 device and it does not have LLDP support.
- **dot3at**–Use this mode if the device is a Class 4 device capable of figuring out power requirements through 2-event classification or LLDP. If the switch supports UPoE and the PD, over an LLDP connection, requests power above 30 watts, UPoE can support power up to 60 watts.
- **upoe**–Use this mode to force power to be delivered using 4 pairs of the cable up to 60 watts without LLDP.

Note: UPoE is supported on the M6100 series switches only.

Default	dot3at
Format	poe high-power {legacy | pre-dot3at | dot3at | upoe}
Mode	Interface Config

no poe high-power

Use this command to disable the high-power mode. The port will support only IEEE 902.3af devices.

This command works on a global basis or per interface.

Format	no poe high-power
Mode	Interface Config

poe power limit

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, and up to 60 watts, if UPoE is supported. Therefore, the range is 3000–60000.

Note: UPoE is supported on the M6100 series switches only.

Default	User-defined, with a maximum of 60 watts if UPoE is supported.
Format	`poe power limit {class-based | none | user-defined` *`maximum-power`*`}`
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	`no poe power limit [user-defined]`
Mode	Global Config Interface Config

poe power management

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

Use this command to set the power management mode to the default.

Format	no poe power management {*unit* | all}
Mode	Global Config

poe priority

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. There are four options:

- Crit—Critical priority
- High—High priority
- Medium—Medium priority
- Low—Low priority

Default	Low
Format	poe priority {Crit | High | Medium | Low}
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

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	`poe reset`
Mode	Global Config Interface Config

poe timer schedule name

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 1094.

Format	`poe timer schedule` *`name`*
Mode	Interface Config

no poe timer schedule name

Use this command to detach the schedule from the port.

Format	`no poe timer schedule`
Mode	Interface Config

poe usagethreshold

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	poe usagethreshold {*unit* | all} *percentage*
Mode	Global Config

no poe usagethreshold

Use this command to set the usage threshold to a default value.

Format	no poe usagethreshold {*unit* | all}
Mode	Global Config

poe traps

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	poe traps
Mode	Global Config

no poe traps

Use this command to disable logging the PoE traps.

Format	no poe traps
Mode	Global Config

show poe

Use this command to get global information regarding the PoE status.

Format	show poe
Mode	Privileged EXEC User EXEC

Term	Definition
Unit	The unit on which PoE module is installed.
Model	The PoE daughter card type. The switch supports two PoE daughter cards: XCM89P and XCM89UP.
Host	The module on which the PoE daughter card is installed.

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	Indicates the maximum amount of power that can be delivered by this PoE unit.
Threshold Power	System 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	Indicates the total amount of power being delivered to all the devices plugged into the switch.
Usage Threshold	Indicates the usage threshold level.
Power Management Mode	Indicates the management mode used by the PoE controller.
Traps	Configures the traps.

Command example:

```
(NETGEAR Switch) #show poe
Unit..................................... 2
Model.................................... UPoE
Host..................................... XCM8948
Firmware Version......................... 1.0.0.2
PSE Main Operational Status.............. ON
Total Power (Main AC).................... 380
Total Power (RPS)........................ 300
Total Power (PD) ........................ 25
Power Source............................. Main AC
Threshold Power.......................... 342
Total Power Consumed..................... 7
Usage Threshold.......................... 90
Power Management Mode.................... Dynamic
Configure port Auto Reset Mode........... Disable
Traps.................................... Enable
```

show poe card

Note: This command is supported on the M6100 series switches only.

This command lists all the UPoE and PoE+ modules in the switch chassis. The host identifies the main module into which the PoE or UPoE daughter card is plugged.

Format	`show poe card [slot-id | all]`
Mode	Privileged EXEC User EXEC

Command example:

```
(NETGEAR Switch) #show poe card all

Slot   Model      Description          Host     Status   PoE FW Version
----   -----      ----------          ------   -------   --------------
1      XCM89P    ProSafe PoE+ D-Card  XCM8944  Running    1.0
2      XCM89UP   ProSafe UPoE D-Card  XCM8948  Running    1.0
```

show poe mpsm

Note: This command is supported on the M6100 series switches only.

This command displays the Multi Protocol Service Module (MPSM) and power bank values.

Format	`show poe mpsm [slot]`
Mode	Privileged EXEC

Command example:

```
(NETGEAR Switch) # show poe mpsm
Current Active MPSM = 1
Slot      Power Bank
                 Value (W)
  1                 580
  2                 610
  3                 550
```

Command example:

```
(NETGEAR Switch) #show poe mpsm 2
Slot = 2
Current Active MPSM = 1
MPSM Number:                  0         1        2        3        4        5
6         7
Power Bank Value (W):       260      610    1080   1430   1780   2130   2480   2830
```

Note: This command only applies when at least one module has PoE capability

show poe port configuration

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.

Format	`show poe port configuration [port | all]`
Mode	Privileged EXEC User EXEC

Command example:

```
(NETGEAR Switch) #show poe port configuration all

        Admin            Power    Power Limit    High Power         Detection
Intf    Mode   Priority  Limit    Type           Mode               Type
                           (W)
------ ------- -------- ------ -------------- ------------ ---------------------
  0/1  Enable     Low    15.400  User Defined    Disable            Auto
  0/2  Enable     Low    15.400  User Defined    Disable            Auto
```

Command example:

```
(NETGEAR Switch) #show poe port configuration 0/2

        Admin            Power    Power Limit    High Power         Detection
Intf    Mode   Priority  Limit    Type           Mode               Type
                           (W)
------ ------- -------- ------ -------------- ------------ ---------------------
  0/2  Enable     Low    15.400  User Defined   Disable            Auto
```

show poe port info

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.

Format	`show poe port info [port | all]`
Mode	Privileged EXEC User EXEC

Term	Definition
Intf	Interface on which PoE is configured.
Class	Class of the powered device according to the IEEE802.3af and IEEE802.3at definition. Class Usage Max Power (watts) • 0 Default 0.44-12.95 • 1 Optional 0.44-3.84 • 2 Optional 3.84-6.49 • 3 Optional 6.49-12.95 • 4 Optional 12.95-25.5
Power	The power supplied to the powered device (in watts).
Output Current (mA)	The current supplied to the powered device (in mA).
Output Voltage (volts)	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.

Command example:

```
(NETGEAR Switch) #show poe port info all

        High       Max                      Output    Output
Intf    Power      Power    Class    Power    Current   Voltage      Status             Fault
                     (W)              (W)      (mA)       (volt)                         Status
------ -------  -----  -------  ------  -------    -------   ------------------ ----------
  0/1    Yes     32.0   Unknown   00.000   0         00.00      Searching          No Error
```

Command example:

```
(NETGEAR Switch) #show poe port info 0/33

         High     Max                      Output    Output
Intf     Power    Power    Class    Power    Current   Voltage      Status               Fault
                    (W)              (W)      (mA)      (volt)                          Status
------ -------  -----   -------  ------  -------    -------    ------------------  --------
  0/33   No      18.0     2       04.400   84         53.3      Delivering Power     No Error
```

NETGEAR Managed Switch Software Log Messages

18

This chapter lists common log messages that are provided by NETGEAR Managed Switch software, 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 will 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*
- *Chassis*
- *Technologies*
- *O/S Support*

Core

Table 19. BSP Log Messages

Component	Message	Cause
BSP	Event(0xaaaaaaaa)	Switch has restarted.
BSP	Starting code...	BSP initialization complete, starting NETGEAR Managed Switch application.

Table 20. NIM Log Messages

Component	Message	Cause
NIM	NIM: L7_ATTACH out of order for interface unit x slot x port x	Interface creation out of order.
NIM	NIM: Failed to find interface at unit x slot 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 slot x port x	Interface creation out of order.
NIM	NIM: L7_DELETE out of order for interface unit x slot 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 21. 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 22. System Log Messages

Component	Message	Cause
SYSTEM	The size of the `startup-config.cfg` 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 *file name* version *version num*	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 *filename*: same version (*version num*) but the sizes (*version size – expected version size*) 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 *filename* from version *version num* to *version num*	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 = *expected size of file* version = *expected version*	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 23. Trap Mgr Log Message

Component	Message	Cause
Trap Mgr	Link Up/Down: unit/slot/port	An interface changed link state.

Table 24. 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 25. 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 26. 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.

Table 26. RADIUS Log Messages (continued)

Component	Message	Cause
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 27. 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.

Table 27. TACACS+ Log Messages (continued)

Component	Message	Cause
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 28. LLDP Log Message

Component	Message	Cause
LLDP	lldpTask(): invalid message type:xx. xxxxxx:xx	Unsupported LLDP packet received.

Table 29. 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 30. 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.
DHCP6 Client	Failed to add DNS Server xxx to DNS Client.	This message appears when the update of a DNS6 Server address given by the DHCPv6 Server to the DNS6 Client fails.
DHCP6 Client	Failed to add Domain name xxx to DNS Client.	This message appears when the update of a DNS6 Domain name info given by the DHCPv6 Server to the DNS6 Client fails.

Table 31. DHCPv4 Client Log Messages

Component	Message	Cause
DHCP4 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.
DHCP4 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.
DHCP4 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.
DHCP4 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.
DHCP4 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 32. SNMP Log Message

Component	Message	Cause
SNMP	EDB Callback: Unit Join: x.	A new blade has joined the chassis.

Table 33. 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	*ConnectionType* EmWeb socket accept() failed: errno	Socket accept failure for the specified connection type.

Table 33. EmWeb Log Messages (continued)

Component	Message	Cause
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:recvBufCnt 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 34. 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 35. 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 36. 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 37. 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	sshdApiCnfgrCommand: Failed calling sshdIssueCmd.	Failed to send the message to the SSHD message queue.

Table 38. 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	ssltApiCnfgrCommand: 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 SSLcertificate from specified file. XXXX indicates the file from where the certificate is being read.

Table 38. SSLT Log Messages

Component	Message	Cause
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 39. 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 40. 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	protectedPortCnfgrInitPhase1Process: Unable to create r/w lock for protected Port	This appears when protectedPortCfgRWLock Fails.
Protected Ports	protectedPortCnfgrInitPhase2Process: 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.

Table 40. Protected Ports Log Messages (continued)

Component	Message	Cause
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 41. 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	vlanIpSubnetCnfgrInitPhase1Process: Unable to create r/w lock for vlanIpSubnet	This appears when a read/write lock creations fails.
IP subnet VLANs	vlanIpSubnetCnfgrInitPhase2Process: Unable to register for VLAN change callback	This appears when this component unable to register for vlan change notifications.
IP subnet VLANs	vlanIpSubnetCnfgrFiniPhase1Process: 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.
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 42. 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	vlanMacCnfgrInitPhase1Process: 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.

Table 42. Mac-based VLANs Log Messages (continued)

Component	Message	Cause
MAC based VLANs	vlanMacCnfgrFiniPhase1Process: 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 43. 802.1X Log Messages

Component	Message	Cause
802.1X	*function*: Failed calling dot1xIssueCmd	802.1X message queue is full.
802.1X	*function:* EAP message not received from server	RADIUS server did not send required EAP message.
802.1X	*function*: Out of System buffers	802.1X cannot process/transmit message due to lack of internal buffers.
802.1X	*function*: could not set state to *authorized/unauthorized*, intf xxx	DTL call failed setting authorization state of the port.
802.1X	dot1xApplyConfigData: Unable to *enable/disable* 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	*function*: failed sending terminate cause, intf xxx	Failed sending accounting stop to RADIUS server.

Table 44. IGMP Snooping Log Messages

Component	Message	Cause
IGMP Snooping	*function*: 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.

Table 44. IGMP Snooping Log Messages (continued)

Component	Message	Cause
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	snoopCnfgrInitPhase1Process: Error allocating small buffers	Could not allocate buffers for small IGMP packets.
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating large buffers	Could not allocate buffers for large IGMP packets.

Table 45. GARP/GVRP/GMRP Log Messages

Component	Message	Cause
GARP/GVRP/ GMRP	garpSpanState, garpIfStateChange, GarpIssueCmd, garpDot1sChangeCallBack, garpApiCnfgrCommand, 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.
GARP/GVRP/ GMRP	garpMapIntfIsConfigurable, gmrpMapIntfIsConfigurable: Error accessing GARP/GMRP config data for interface %d in garpMapIntfIsConfigurable.	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 46. 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 47. 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 48. Double VLAN Tag Log Message

Component	Message	Cause
Double Vlan Tag	dvlantagIntfIsConfigurable: 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 49. IPv6 Provisioning Log Message

Component	Message	Cause
IPV6 Provisioning	ipv6ProvIntfIsConfigurable: 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 50. MFDB Log Message

Component	Message	Cause
MFDB	mfdbTreeEntryUpdate: entry does not exist	Trying to update a non existing entry.

Table 51. 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	dot1qMapIntfIsConfigurable: Error accessing DOT1Q config data for interface %d in dot1qMapIntfIsConfigurable.	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.
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.

Table 51. 802.1Q Log Messages (continued)

Component	Message	Cause
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.
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.

Table 51. 802.1Q Log Messages (continued)

Component	Message	Cause
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 52. 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 53. Port Mac Locking Log Message

Component	Message	Cause
Port Mac Locking	pmlMapIntfIsConfigurable: Error accessing PML config data for interface %d in pmlMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.

Table 54. Protocol-based VLANs Log Messages

Component	Message	Cause
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register NIM callback	Appears when nimRegisterIntfChange fails to register pbVlan for link state changes.
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with VLANs	Appears when VLANRegisterForChange fails to register pbVlan for VLAN changes.
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with nvStore	Appears when nvStoreRegister fails to register save and restore functions for configuration save.

QoS

Table 55. 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 *name*, 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 *number*	The system was unable to send an SNMP trap for this ACL rule which contains a logging attribute.
ACL	IP ACL *number*: 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 56. CoS Log Message

Component	Message	Cause
COS	cosCnfgrInitPhase3Process: 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 57. 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 *name*, interface *x*, direction *y*	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 58. 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 59. OSPFv2 Log Messages

Component	Message	Cause
OSPFv2	Best route client deregistration failed for OSPF Redist	OSPFv2 registers with the IPv4 routing table manager (“RTO”) to be notified of best route changes. There are cases where OSPFv2 deregisters more than once, causing the second deregistration to fail. The failure is harmless.
OSPFv2	XX_Call() failure in _checkTimers for thread 0x869bcc0	An OSPFv2 timer has fired but the message queue that holds the event has filled up. This is normally a fatal error.
OSPFv2	Warning: OSPF LSDB is 90% full (22648 LSAs).	OSPFv2 limits the number of Link State Advertisements (LSAs) that can be stored in the link state database (LSDB). When the database becomes 90 or 95 percent full, OSPFv2 logs this warning. The warning includes the current size of the database.
OSPFv2	The number of LSAs, 25165, in the OSPF LSDB has exceeded the LSDB memory allocation.	When the OSPFv2 LSDB becomes full, OSPFv2 logs this message. OSPFv2 reoriginates its router LSAs with the metric of all non-stub links set to the maximum value to encourage other routers to not compute routes through the overloaded router.

Table 59. OSPFv2 Log Messages (continued)

Component	Message	Cause
OSPFv2	Dropping the DD packet because of MTU mismatch	OSPFv2 ignored a Database Description packet whose MTU is greater than the IP MTU on the interface where the DD was received.
OSPFv2	LSA Checksum error in LsUpdate, dropping LSID 1.2.3.4 checksum 0x1234.	OSPFv2 ignored a received link state advertisement (LSA) whose checksum was incorrect.

Table 60. OSPFv3 Log Messages

Component	Message	Cause
OSPFv3	Best route client deregistration failed for OSPFv3 Redist	OSPFv3 registers with the IPv6 routing table manager (“RTO6”) to be notified of best route changes. There are cases where OSPFv3 deregisters more than once, causing the second deregistration to fail. The failure is harmless.
OSPFv3	Warning: OSPF LSDB is 90% full (15292 LSAs).	OSPFv3 limits the number of Link State Advertisements (LSAs) that can be stored in the link state database (LSDB). When the database becomes 90 or 95 percent full, OSPFv3 logs this warning. The warning includes the current size of the database.
OSPFv3	The number of LSAs, 16992, in the OSPF LSDB has exceeded the LSDB memory allocation.	When the OSPFv3 LSDB becomes full, OSPFv3 logs this message. OSPFv3 reoriginates its router LSAs with the R-bit clear indicating that OSPFv3 is overloaded.
OSPFv3	LSA Checksum error detected for LSID 1.2.3.4 checksum 0x34f5. OSPFv3 Database may be corrupted.	OSPFv3 periodically verifies the checksum of each LSA in memory. OSPFv3 logs this.

Table 61. 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 62. VRRP Log Messages

Component	Message	Cause
VRRP	VRRP packet of size xxx dropped. Min VRRP packet size is xxx; Max VRRP packet size is xxx.	This message appears when there is flood of VRRP messages in the network.
VRRP	VR xxx on interface xxx started as xxx.	This message appears when the Virtual router is started in the role of a Master or a Backup.
VRRP	This router is the IP address owner for virtual router xxx on interface xxx. Setting the virtual router priority to xxx.	This message appears when the address ownership status for a specific VR is updated. If this router is the address owner for the VR, set the VR's priority to MAX priority (as per RFC 3768). If the router is no longer the address owner, revert the priority.

Table 63. 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 64. 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 65. 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.

Table 65. IGMP/MLD Log Messages

Component	Message	Cause
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 66. 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 67. 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.
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.

Table 67. PIM-SM Log Messages (continued)

Component	Message	Cause
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 68. 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.
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.

Table 68. PIM-DM Log Messages (continued)

Component	Message	Cause
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.
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.

Table 69. DVMRP Log Messages

Component	Message	Cause
DVMRP	DVMRP Heap memory initialization is Failed for the specified address family.	This message appears when trying to enable DVMRP Protocol
DVMRP	DVMRP Heap memory de-initialization is Failed for the specified address family.	This message appears when trying to disable DVMRP Protocol. As a result of this, the subsequent attempts to enable/disable DVMRP will also fail.

Table 69. DVMRP Log Messages (continued)

Component	Message	Cause
DVMRP	DVMRP protocol initialization sequence Failed.	This could be due to the non-availability of some resources. This message appears when trying to enable DVMRP Protocol.
DVMRP	DVMRP All Routers Address - xxx Delete from the DTL Mcast List Failed for intf – xxx.	DMVRP All Routers Address deletion from the local multicast list Failed. As a result of this, DVMRP Multicast packets are still received at the application though DVMRP is disabled.
DVMRP	Mcast Forwarding Mode Disable Failed for intf – xxx.	The Multicast Forwarding mode Disable Failed for this routing interface.
DVMRP	DVMRP All Routers Address - xxx Add to the DTL Mcast List Failed for intf – xxx.	DMVRP All Routers Address addition to the local multicast list Failed. As a result of this, DVMRP Multicast packets with this address will not be received at the application.
DVMRP	Mcast Forwarding Mode Enable Failed for intf – xxx.	The Multicast Forwarding mode Enable Failed for this routing interface. As a result of this, the ability to forward Multicast packets does not function on this interface.
DVMRP	DVMRP Probe Control message Send Failed on rtrIfNum – xxx.	DVMRP Probe control message send failed. This could mostly be because of a Failure return status of the socket call sendto(). As a result of this, the DVMRP neighbor could be lost in the neighboring DVMRP routers.
DVMRP	DVMRP Prune Control message Send Failed; rtrIfNum – xxx.	Neighbor - %s, SrcAddr - %s, GrpAddr - %s DVMRP Prune control message send failed. This could mostly be because of a Failure return status of the socket call sendto(). As a result of this, the unwanted multicast traffic is still received and forwarded.
DVMRP	DVMRP Probe Control message Send Failed on rtrIfNum –xxx.	DVMRP Probe control message send failed. This could mostly be because of a Failure return status of the socket call sendto(). As a result of this, the DVMRP neighbor could be lost in the neighboring DVMRP routers.

Chassis

Table 70. EDB Log Message

Component	Message	Cause
EDB	EDB Callback: Unit Join: *num*.	Unit *num* has joined the chassis.

Technologies

Table 71. Error Messages

Component	Message	Cause
OS	Invalid USP unit = x, slot = 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 it's 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.
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.

Table 71. Error Messages (continued)

Component	Message	Cause
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.
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.

Table 71. Error Messages (continued)

Component	Message	Cause
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 72. BSP Log Message

Component	Message	Cause
BSP	rc = 10	Second message logged at bootup, right after *Starting code…. Always* logged.

Table 73. 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	l3intfAddRoute: Failed to Add Route – or – l3intfDeleteRoute: 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).

Table 73. OSAPI Log Messages (continued)

Component	Message	Cause
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.
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 VRRP IP or MAC address(es) to a network interface.

Command List

{deny | permit} (IP ACL) 1078
{deny | permit} (IPv6) 1088
{deny | permit} (MAC ACL) 1068
1583compatibility 742
aaa accounting 128
aaa authentication dot1x default 434
aaa authentication enable 104
aaa authentication login 103
aaa authorization 106
aaa ias-user username 126
aaa session-id 127
absolute 1095
access-list 1073
accounting 131
acl-trapflags 1083
activate 884
addport 477
address prefix (IPv6) 1013
address-family 883
address-family ipv6 839
aggregate-address 840
area default-cost (OSPF) 743
area default-cost (OSPFv3) 967
area nssa (OSPF) 743
area nssa (OSPFv3) 967
area nssa default-info-originate (OSPF) 743
area nssa default-info-originate (OSPFv3) 968
area nssa no-redistribute (OSPF) 744
area nssa no-redistribute (OSPFv3) 968
area nssa no-summary (OSPF) 744
area nssa no-summary (OSPFv3) 969
area nssa translator-role (OSPF) 744
area nssa translator-role (OSPFv3) 969
area nssa translator-stab-intv (OSPF) 745
area nssa translator-stab-intv (OSPFv3) 969
area range (OSPF) 745
area range (OSPFv3) 970
area stub (OSPF) 747

area stub (OSPFv3) 971
area stub no-summary (OSPF) 747
area stub no-summary (OSPFv3) 971
area virtual-link (OSPF) 748
area virtual-link (OSPFv3) 971
area virtual-link authentication 748
area virtual-link dead-interval (OSPF) 749
area virtual-link dead-interval (OSPFv3) 972
area virtual-link hello-interval (OSPF) 749
area virtual-link hello-interval (OSPFv3) 972
area virtual-link retransmit-interval (OSPF) 749
area virtual-link retransmit-interval (OSPFv3) 973
area virtual-link transmit-delay (OSPF) 750
area virtual-link transmit-delay (OSPFv3) 973
arp 661
arp access-list 538
arp cachesize 662
arp dynamicrenew 662
arp purge 663
arp resptime 663
arp retries 664
arp timeout 664
assign-queue 1054
authentication enable 443
authentication order 443
authentication priority 444
authentication restart 444
authentication timeout 810
authorization commands 108
authorization exec 108
authorization exec default 109
authorization network radius 146
auto-cost (OSPF) 750
auto-cost (OSPFv3) 974
auto-negotiate 357
auto-negotiate all 358
auto-summary 797
auto-voip 1097
auto-voip oui 1098
auto-voip oui-based priority 1098
auto-voip protocol-based 1099
auto-voip vlan 1100
background-color 821
bandwidth 762

bgp aggregate-different-meds (BGP Router Config) 841
bgp aggregate-different-meds (IPv6 Address Family Config) 841
bgp always-compare-med (BGP Router Config) 842
bgp always-compare-med (IPv6 Address Family Config) 842
bgp client-to-client reflection (BGP Router Config) 843
bgp client-to-client reflection (IPv6 Address Family Config) 844
bgp cluster-id 845
bgp default local-preference 845
bgp fast-external-failover 846
bgp fast-internal-failover 846
bgp log-neighbor-changes 847
bgp maxas-limit 847
bgp router-id 848
block 820
boot auto-copy-sw (for chassis firmware synchronization) 38
boot auto-copy-sw (for stack firmware synchronization) 61
boot auto-copy-sw allow-downgrade (for chassis firmware synchronization) 38
boot auto-copy-sw allow-downgrade (for stack firmware synchronization) 62
boot auto-copy-sw trap (for chassis firmware synchronization) 38
boot auto-copy-sw trap (for stack firmware synchronization) 62
boot autoinstall 172
boot host autoreboot 173
boot host autosave 173
boot host dhcp 172
boot host retrycount 172
boot system 177
bootfile 249
bootpdhcprelay cidoptmode 731
bootpdhcprelay maxhopcount 732
bootpdhcprelay minwaittime 732
bridge aging-time 607
cablestatus 306
capability opaque 751
captive-portal 808
captive-portal client deauthenticate 827
capture {file | remote | line} 265
capture file size 266
capture line wrap 266
capture remote port 266
capture start 264
capture stop 265
chassis 27
chassis-status sample-mode 27
class 1055
class-map 1045

class-map rename 1046
classofservice dot1p-mapping 1035
classofservice ip-dscp-mapping 1035
classofservice traffic-class-group 631
classofservice trust 1036
clear (Captive Portal Instance Config) 821
clear aaa ias-users 130
clear accounting statistics 133
clear arp-cache 665
clear arp-switch 665
clear authentication authentication-history 449
clear authentication statistics 448
clear captive-portal users 836
clear checkpoint statistics (for chassis configuration) 42
clear checkpoint statistics (for stack configuration) 67
clear config 226
clear counters 226
clear dhcp l2relay statistics interface 523
clear dot1x authentication-history 435
clear dot1x statistics 435
clear eventlog 217
clear fip-snooping statistics 654
clear green-mode statistics 329
clear host 262
clear igmpsnooping 227
clear ip address-conflict-detect 264
clear ip arp inspection statistics 540
clear ip bgp 888
clear ip bgp counters 889
clear ip community-list 921
clear ip dhcp binding 254
clear ip dhcp conflict 255
clear ip dhcp server statistics 254
clear ip dhcp snooping binding 533
clear ip dhcp snooping statistics 533
clear ip helper statistics 735
clear ip mroute 1116
clear ip ospf 751
clear ip ospf configuration 752
clear ip ospf counters 752
clear ip ospf neighbor 752
clear ip ospf neighbor interface 752
clear ip ospf redistribution 752
clear ip ospf stub-router 774

clear ip prefix-list 714
clear ip route 689
clear ipv6 dhcp 1021
clear ipv6 dhcp binding 1021
clear ipv6 dhcp snooping binding 1031
clear ipv6 dhcp snooping statistics 1031
clear ipv6 mld counters 1177
clear ipv6 mld traffic 1177
clear ipv6 mroute 1156
clear ipv6 neighbors 953
clear ipv6 ospf 974
clear ipv6 ospf configuration 975
clear ipv6 ospf counters 975
clear ipv6 ospf neighbor 975
clear ipv6 ospf neighbor interface 975
clear ipv6 ospf redistribution 976
clear ipv6 ospf stub-router 993
clear ipv6 prefix-list 714
clear ipv6 route counters 962
clear ipv6 statistics 966
clear isdp counters 611
clear isdp table 611
clear lldp remote-data 584
clear lldp statistics 584
clear logging buffered 217
clear logging email statistics 221
clear mac-addr-table 227
clear mldsnooping 571
clear mmrp statistics 470
clear mvrp 474
clear network ipv6 dhcp statistics 1022
clear pass 227
clear port-channel all counters 495
clear port-channel counters 495
clear priority-flow-control statistics 657
clear radius statistics 435
clear serviceport ipv6 dhcp statistics 1022
clear traplog 227
clear vlan 227
clear vpc statistics 507
client-identifier 246
client-name 246
clock set 241
clock summer-time date 242
clock summer-time recurring 242

clock timezone 243
configuration (for captive portal) 813
configure 78
conform-color 1055
connect-retry-interval 884
console 303
copy 231
copy (pre-login banner) 167
cos-queue min-bandwidth 1036
cos-queue random-detect 1037
cos-queue strict 1037
crypto certificate generate 88
crypto key generate dsa 89
crypto key generate rsa 89
dampening 768
debounce-time 621
debug aaa accounting 267
debug aaa authorization 267
debug arp 268
debug authentication 269
debug auto-voip 269
debug clear 269
debug console 269
debug crashlog 270
debug dcbx packet 271
debug debug-config 271
debug dhcp packet 272
debug dot1x packet 272
debug environment 208
debug fip-snooping packet 273
debug i2c 209
debug igmpsnooping packet 274
debug igmpsnooping packet receive 275
debug igmpsnooping packet transmit 274
debug ip acl 276
debug ip bgp (BGP commands) 889
debug ip bgp (serviceability packet tracing) 276
debug ip dvmrp packet 277
debug ip igmp packet 278
debug ip mcache packet 278
debug ip pimdm packet 279
debug ip pimsm packet 279
debug ip vrrp 280
debug ipv6 dhcp 280

debug ipv6 mcache packet 281
debug ipv6 mld packet 281
debug ipv6 ospfv3 packet 282
debug ipv6 pimsm packet 282
debug isdp packet 616
debug lacp packet 282
debug mldsnooping packet 283
debug ospf packet 284
debug ping packet 286
debug rip packet 287
debug sflow packet 288
debug spanning-tree bpdu 288
debug spanning-tree bpdu receive 289
debug spanning-tree bpdu transmit 290
debug tacacs 291
debug transfer 291
debug udld events 291
debug udld packet receive 292
debug udld packet transmit 292
debug vpc core 508
debug vpc peer detection 509
debug vpc peer-keepalive 508
debug vpc peer-link control-message async 508
debug vpc peer-link control-message bulk 508
debug vpc peer-link control-message ckpt 509
debug vpc peer-link data-message 508
default metric (BGP Router Config) 849
default metric (IPv6 Address Family Config) 850
default-information originate (BGP Router Config) 848
default-information originate (IPv6 Address Family Config) 849
default-information originate (OSPF) 753
default-information originate (OSPFv3) 976
default-information originate (RIP) 797
default-metric (OSPF) 753
default-metric (OSPFv3) 976
default-metric (RIP) 798
default-router 247
delete 177
deleteport (Global Config) 478
deleteport (Interface Config) 477
deny ip-source 91
deny priority 92
deny service 92
description (Interface Config) 358
description (Peer Template Config) 885

dhcp client vendor-id-option 524
dhcp client vendor-id-option-string 524
dhcp l2relay 517
dhcp l2relay circuit-id vlan 517
dhcp l2relay remote-id subscription 517
dhcp l2relay remote-id vlan 518
dhcp l2relay subscription 519
dhcp l2relay trust 519
dhcp l2relay vlan 519
diffserv 1044
dir 204
dir usb 310
disconnect 102
distance (BGP Router Config) 850
distance BGP (BGP Router Config) 852
distance BGP (IPv6 Address Family Config) 852
distance ospf (OSPF) 753
distance ospf (OSPFv3) 977
distance rip 798
distribute-list out (OSPF) 754
distribute-list out (RIP) 798
distribute-list prefix in 853
distribute-list prefix out (BGP) 854
dns-server 247
dns-server (IPv6) 1014
do (Captive Portal Instance mode) 819
do (Privileged EXEC commands) 72
domain-name 249
domain-name (IPv6) 1014
domain-name enable 250
dos-control all 598
dos-control firstfrag 599
dos-control icmpfrag 605
dos-control icmpv4 604
dos-control icmpv6 605
dos-control l4port 600
dos-control sipdip 598
dos-control smacdmac 601
dos-control tcpfinurgpsh 604
dos-control tcpflag 600
dos-control tcpflagseq 602
dos-control tcpfrag 599
dos-control tcpoffset 602
dos-control tcpport 601

dos-control tcpsyn 603
dos-control tcpsynfin 603
dos-control udpport 602
dot1x dynamic-vlan enable 436
dot1x eapolflood 436
dot1x guest-vlan 436
dot1x initialize 437
dot1x mac-auth-bypass 439
dot1x max-req 437
dot1x max-users 437
dot1x pae 456
dot1x port-control 438
dot1x port-control all 438
dot1x re-authenticate 439
dot1x re-authentication 440
dot1x supplicant max-start 457
dot1x supplicant port-control 456
dot1x supplicant timeout auth-period 458
dot1x supplicant timeout held-period 457
dot1x supplicant timeout start-period 457
dot1x supplicant user 458
dot1x system-auth-control 440
dot1x system-auth-control monitor 440
dot1x timeout 441
dot1x unauthenticated-vlan 442
dot1x user 442
drop 1054
dvlan-tunnel ethertype (Interface Config) 413
dvlan-tunnel ethertype primary-tpid 413
enable (BGP) 854
enable (Captive Portal Config Mode) 808
enable (Captive Portal Instance) 814
enable (OSPF) 742
enable (OSPFv3) 977
enable (Privileged EXEC access) 72
enable (RIP) 796
enable authentication 110
enable password (Privileged EXEC) 119
encapsulation 674
environment temprange 208
environment trap 208
erase factory-defaults 174
erase stack-config 174
erase startup-config 173
exception core-file 296

exception dump compression 295
exception dump filepath 295
exception dump ftp-server 293
exception dump nfs 294
exception dump stack-ip-address add 296
exception dump stack-ip-address protocol 295
exception dump stack-ip-address remove 296
exception dump tftp-server 294
exception nmi 297
exception protocol 293
exception switch-chip-register 297
exit-overflow-interval (OSPF) 754
exit-overflow-interval (OSPFv3) 977
external-lsdb-limit (OSPF) 755
external-lsdb-limit (OSPFv3) 978
ezconfig 69
feature fip-snooping 637
feature vpc 496
file verify 235
filedescr 178
fip-snooping enable 638
fip-snooping fc-map 638
fip-snooping port-mode 639
flowcontrol 423
foreground-color 821
green-mode eee 322
green-mode eee tx-idle-time 323
green-mode eee tx-wake-time 323
green-mode eee-lpi-history max-samples 325
green-mode eee-lpi-history sampling-interval 324
green-mode energy-detect 322
group 815
hardware-address 247
host 248
hostname 168
hostroutesaccept 800
http port 808
https port 809
idle-timeout 819
initiate failover (for chassis configuration) 41
initiate failover (for stack configuration) 66
interface (Captive Portal Instance) 820
interface (Global Config) 357
interface lag 486

interface loopback 931
interface tunnel 929
interface vlan 721
ip access-group 1082
ip access-list 1077
ip access-list rename 1077
ip address 668
ip address dhcp 669
ip address-conflict-detect run 263
ip arp inspection filter 537
ip arp inspection limit 537
ip arp inspection trust 536
ip arp inspection validate 535
ip arp inspection vlan 535
ip arp inspection vlan logging 536
ip as-path access-list 917
ip bgp fast-external-failover 855
ip bgp-community new-format 918
ip community-list 919
ip cpu-priority 71
ip default-gateway 670
ip dhcp bootp automatic 253
ip dhcp conflict logging 254
ip dhcp excluded-address 252
ip dhcp ping packets 252
ip dhcp pool 245
ip dhcp snooping 525
ip dhcp snooping binding 527
ip dhcp snooping database 526
ip dhcp snooping database write-delay (DHCP) 526
ip dhcp snooping database write-delay (DHCPv6) 1024
ip dhcp snooping limit 527
ip dhcp snooping log-invalid 528
ip dhcp snooping trust 528
ip dhcp snooping verify mac-address 526
ip dhcp snooping vlan 525
ip domain list 259
ip domain lookup 258
ip domain name 258
ip domain retry 261
ip domain timeout 261
ip dvmrp (Global Config) 1117
ip dvmrp (Interface Config) 1118
ip dvmrp metric 1117
ip dvmrp trapflags 1118

ip helper enable 738
ip helper-address (Global Config) 735
ip helper-address (Interface Config) 736
ip host 260
ip http accounting exec, ip https accounting exec 94
ip http authentication 94
ip http java 97
ip http secure-port 100
ip http secure-protocol 100
ip http secure-server 97
ip http secure-session hard-timeout 99
ip http secure-session maxsessions 99
ip http secure-session soft-timeout 99
ip http server 96
ip http session hard-timeout 97
ip http session maxsessions 98
ip http session soft-timeout 98
ip https authentication 95
ip icmp echo-reply 805
ip icmp error-interval 805
ip igmp 1137
ip igmp header-validation 1138
ip igmp last-member-query-count 1138
ip igmp last-member-query-interval 1139
ip igmp query-interval 1139
ip igmp query-max-response-time 1140
ip igmp robustness 1140
ip igmp startup-query-count 1141
ip igmp startup-query-interval 1141
ip igmp version 1138
ip igmp-proxy 1145
ip igmp-proxy reset-status 1146
ip igmp-proxy unsolicit-rprt-interval 1146
ip irdp 715
ip irdp address 715
ip irdp holdtime 716
ip irdp maxadvertinterval 716
ip irdp minadvertinterval 717
ip irdp multicast 717
ip irdp preference 717
ip local-proxy-arp 662
ip management 73
ip mcast boundary 1110
ip mroute 1110

ip mtu 673
ip multicast 1111
ip multicast ttl-threshold 1111
ip name server 259
ip name source-interface 260
ip netdirbcast 673
ip ospf area 762
ip ospf authentication 763
ip ospf cost 763
ip ospf database-filter all out 763
ip ospf dead-interval 764
ip ospf hello-interval 764
ip ospf mtu-ignore 767
ip ospf network 765
ip ospf prefix-suppression 765
ip ospf priority 766
ip ospf retransmit-interval 766
ip ospf transmit-delay 767
ip pim 1123
ip pim bsr-border 1124
ip pim bsr-candidate 1124
ip pim dense 1122
ip pim dr-priority 1125
ip pim hello-interval 1123
ip pim join-prune-interval 1126
ip pim rp-address 1127
ip pim rp-candidate 1127
ip pim sparse 1122
ip pim ssm 1128
ip pim-trapflags 1129
ip policy route-map 691
ip prefix-list 692
ip prefix-list description 694
ip proxy-arp 661
ip redirects 804
ip rip 797
ip rip authentication 799
ip rip receive version 799
ip rip send version 800
ip route 671
ip route default 672
ip route distance 672
ip routing 667
ip ssh 86
ip ssh protocol 86

ip ssh server enable 86
ip telnet server enable 81
ip unreachables 804
ip verify binding 527
ip verify source 529
ip vrrp (Global Config) 722
ip vrrp (Interface Config) 722
ip vrrp accept-mode 724
ip vrrp authentication 724
ip vrrp ip 723
ip vrrp mode 723
ip vrrp preempt 725
ip vrrp priority 725
ip vrrp timers advertise 726
ip vrrp track interface 726
ip vrrp track ip route 727
ipv6 access-list 1087
ipv6 access-list rename 1088
ipv6 address 934
ipv6 address autoconfig 935
ipv6 address dhcp 935
ipv6 cpu-priority 71
ipv6 dhcp client pd 1011
ipv6 dhcp pool 1012
ipv6 dhcp relay destination 1012
ipv6 dhcp server 1011
ipv6 dhcp snooping 1023
ipv6 dhcp snooping binding 1024
ipv6 dhcp snooping database 1024
ipv6 dhcp snooping limit 1026
ipv6 dhcp snooping log-invalid 1025
ipv6 dhcp snooping trust 1025
ipv6 dhcp snooping verify mac-address 1023
ipv6 dhcp snooping vlan 1023
ipv6 enable 933
ipv6 hop-limit 933
ipv6 host 261
ipv6 icmp error-interval 946
ipv6 mld last-member-query-count 1173
ipv6 mld last-member-query-interval 1172
ipv6 mld query-interval 1171
ipv6 mld query-max-response-time 1172
ipv6 mld router 1171
ipv6 mld version 1173

ipv6 mld-proxy 1178
ipv6 mld-proxy reset-status 1178
ipv6 mld-proxy unsolicit-rprt-interval 1178
ipv6 mroute 1153
ipv6 mtu 937
ipv6 nd dad attempts 938
ipv6 nd managed-config-flag 938
ipv6 nd ns-interval 938
ipv6 nd other-config-flag 939
ipv6 nd prefix 942
ipv6 nd ra hop-limit unspecified 940
ipv6 nd ra-interval 939
ipv6 nd ra-lifetime 940
ipv6 nd reachable-time 941
ipv6 nd router-preference 941
ipv6 nd suppress-ra 941
ipv6 neighbor 943
ipv6 neighbors dynamicrenew 943
ipv6 nud 944
ipv6 ospf area 983
ipv6 ospf cost 983
ipv6 ospf dead-interval 984
ipv6 ospf hello-interval 984
ipv6 ospf link-lsa-suppression 985
ipv6 ospf mtu-ignore 985
ipv6 ospf network 986
ipv6 ospf prefix-suppression 986
ipv6 ospf priority 987
ipv6 ospf retransmit-interval 987
ipv6 ospf transmit-delay 988
ipv6 pim 1158
ipv6 pim bsr-border 1159
ipv6 pim bsr-candidate 1159
ipv6 pim dense 1157
ipv6 pim dr-priority 1160
ipv6 pim hello-interval 1158
ipv6 pim join-prune-interval 1161
ipv6 pim rp-address 1162
ipv6 pim rp-candidate 1162
ipv6 pim sparse 1157
ipv6 pim ssm 1163
ipv6 prefix-list (IPv6 routing commands) 944
ipv6 prefix-list (routing policy commands) 694
ipv6 redirects 805
ipv6 route 935

ipv6 route distance 936
ipv6 router ospf 967
ipv6 traffic-filter 1092
ipv6 unicast-routing 933
ipv6 unreachables 946
ipv6 unresolved-traffic 946
ipv6 verify binding 1027
ipv6 verify source 1026
iscsi aging time 1102
iscsi cos 1103
iscsi enable 1104
iscsi target port 1105
isdp advertise-v2 610
isdp enable 610
isdp holdtime 610
isdp run 609
isdp timer 610
key (TACACS Config) 163
keystring (TACACS Config) 163
lacp actor admin key 479
lacp actor admin state 481
lacp actor admin state individual 479
lacp actor admin state longtimeout 480
lacp actor admin state passive 480
lacp actor port priority 481
lacp admin key 478
lacp collector max-delay 478
lacp partner admin key 482
lacp partner admin state individual 482
lacp partner admin state longtimeout 483
lacp partner admin state passive 483
lacp partner port id 484
lacp partner port priority 484
lacp partner system priority 485
lacp partner system-id 485
lease 248
length 206
line 79
lldp dcbx port-role 626
lldp dcbx version 624
lldp med 590
lldp med all 591
lldp med confignotification 590
lldp med confignotification all 591

lldp med faststartrepeatcount 591
lldp med transmit-tlv 590
lldp med transmit-tlv all 592
lldp notification 583
lldp notification-interval 583
lldp receive 581
lldp timers 582
lldp tlv-select dcbxp 625
lldp transmit 581
lldp transmit-mgmt 583
lldp transmit-tlv 582
llpf 467
locale 819
log-adjacency-changes 755
logging buffered 209
logging buffered wrap 210
logging cli-command 210
logging console 210
logging email 217
logging email from-addr 219
logging email logtime 219
logging email message-type subject 219
logging email message-type to-addr 218
logging email test message-type 220
logging email urgent 218
logging host 211
logging host reconfigure 211
logging host remove 212
logging persistent 298
logging port 212
logging syslog 212
logging syslog port 213
logging syslog source-interface 213
logging traps 220
login authentication 118
logout 228
mac access-group 1070
mac access-list extended 1067
mac access-list extended rename 1068
macfilter 512
macfilter adddest 513
macfilter adddest all 514
macfilter addsrc 515
macfilter addsrc all 515
mail-server 222

management access-class 92
management access-list 90
mark cos 1056
mark cos-as-sec-cos 1056
mark ip-dscp 1057
mark ip-precedence 1057
match any 1046
match as-path 697
match class-map 1047
match community 697
match cos 1047
match destination-address mac 1048
match dstip 1048
match dstip6 1049
match dstl4port 1049
match ethertype 1046
match ip address 698
match ip address {access-list-number | access-list-name} 699
match ip dscp 1049
match ip precedence 1050
match ip tos 1050
match ip6flowlbl 1051
match ipv6 address 701
match length 702
match mac-list 702
match protocol 1051
match secondary-cos 1048
match secondary-vlan 1053
match source-address mac 1051
match srcip 1052
match srcip6 1052
match srcl4port 1052
match vlan 1053
max-bandwidth-down 816
max-bandwidth-up 816
maximum-paths (BGP Router Config) 856
maximum-paths (IPv6 Address Family Config) 856
maximum-paths (OSPF) 757
maximum-paths (OSPFv3) 978
maximum-paths igbp (BGP Router Config) 857
maximum-paths igbp (IPv6 Address Family Config) 857
max-input-octets 817
max-metric router-lsa (OSPFv2 Router Configuration) 773
max-metric router-lsa (OSPFv3 Router Configuration) 992

max-output-octets 817
max-total-octets 818
mbuf 299
member (Chassis Global Config) 27
member (Stack Global Config) 44
memory free low-watermark processor 207
mirror 1054
mmrp (Global Config) 469
mmrp (Interface Config) 470
mmrp periodic state machine 469
mode dot1q-tunnel 414
mode dvlan-tunnel 414
monitor session 509
movemanagement (Chassis Global Config) 28
movemanagement (Stack Global Config) 45
mrp 468
mtu 358
mvr 542
mvr group 542
mvr immediate 545
mvr mode 543
mvr querytime 543
mvr type 545
mvr vlan 544
mvr vlan group 546
mvrp (Global Config) 473
mvrp (Interface Config) 474
mvrp periodic state machine 473
name 814
neighbor activate 858
neighbor advertisement-interval (BGP Router Config) 859
neighbor advertisement-interval (IPv6 Address Family Config) 860
neighbor connect-retry-interval 860
neighbor default-originate (BGP Router Config) 861
neighbor default-originate (IPv6 Address Family Config) 862
neighbor description 863
neighbor filter-list (BGP Router Config) 863
neighbor filter-list (IPv6 Address Family Config) 864
neighbor inherit peer 865
neighbor maximum-prefix (BGP Router Config) 866
neighbor maximum-prefix (IPv6 Address Family Config) 866
neighbor next-hop-self (BGP Router Config) 867
neighbor next-hop-self (IPv6 Address Family Config) 868
neighbor password 868
neighbor prefix-list 869

neighbor remote-as 870
neighbor remove-private-as (BGP Router Config) 871
neighbor remove-private-as (IPv6 Address Family Config) 871
neighbor route-map (BGP Router Config) 872
neighbor route-map (IPv6 Address Family Config) 872
neighbor route-reflector-client (BGP Router Config) 873
neighbor route-reflector-client (IPv6 Address Family Config) 874
neighbor send-community 874
neighbor shutdown 875
neighbor timers 876
neighbor update-source 877
netbios-name-server 250
netbios-node-type 251
network (BGP Router Config) 877
network (DHCP Pool Config) 249
network (IPv6 Address Family Config) 878
network area (OSPF) 742
network javamode 75
network mac-address 74
network mac-type 74
network mgmt_vlan 395
next-server 251
no shutdown 886
nsf (OSPF) 771
nsf (OSPFv3) 989
nsf (Stack Global Config) 64
nsf helper 772
nsf helper (OSPFv3) 990
nsf helper strict-lsa-checking (OSPF) 773
nsf helper strict-lsa-checking (OSPFv3) 991
nsf ietf helper disable (OSPF) 772
nsf ietf helper disable (OSPFv3) 991
nsf restart-interval (OSPF) 771
nsf restart-interval (OSPFv3) 989
option 251
passive-interface (OSPF) 758
passive-interface (OSPFv3) 979
passive-interface default 758
passive-interface default (OSPFv3) 979
password (AAA IAS User Config) 129
password (Line Configuration) 118
password (Mail Server Config) 223
password (Peer Template Config) 886
password (User EXEC) 119

passwords aging 121
passwords history 121
passwords lock-out 121
passwords min-length 120
passwords strength exclude-keyword 125
passwords strength maximum consecutive-characters 122
passwords strength maximum repeated-characters 123
passwords strength minimum character-classes 125
passwords strength minimum lowercase-letters 123
passwords strength minimum numeric-characters 124
passwords strength minimum special-characters 124
passwords strength minimum uppercase-letters 123
passwords strength-check 122
peer detection enable 497
peer detection interval 497
peer-keepalive destination 498
peer-keepalive enable 498
peer-keepalive timeout 499
periodic 1096
permit ip host mac host 538
permit ip-source 90
permit priority 91
permit service 91
ping 228
ping ipv6 927
ping ipv6 interface 929
poe 1185
poe detection 1185
poe high-power 1186
poe power limit 1186
poe power management 1187
poe priority 1188
poe reset 1188
poe timer schedule name 1189
poe traps 1190
poe usagethreshold 1189
police-simple 1057
police-single-rate 1058
police-two-rate 1058
policy-map 1059
policy-map rename 1059
port (Mail Server Config) 222
port (TACACS Config) 163
port lacpmode 486
port lacpmode enable all 487

port lacptimeout (Global Config) 488
port lacptimeout (Interface Config) 487
port-channel 477
port-channel adminmode 488
port-channel linktrap 488
port-channel load-balance 489
port-channel local-preference 490
port-channel min-links 490
port-channel name 491
port-channel static 486
port-channel system priority 491
port-security 576
port-security mac-address 577
port-security mac-address move 578
port-security mac-address sticky 578
port-security max-dynamic 576
port-security max-static 577
power auto-rebalance 306
power cycle 309
power rebalance 309
power redundancy 307
power system 307
prefix-delegation (IPv6) 1015
prefix-suppression (Router OSPF Config) 756
prefix-suppression (Router OSPFv3 Config) 756
priority (TACACS Config) 163
priority-flow-control mode 655
priority-flow-control priority 656
private-group name 427
private-vlan 418
process cpu threshold 196
protocol 814
protocol group 402
protocol vlan group 402
protocol vlan group all 403
quit 230
radius accounting mode 146
radius server attribute 4 146
radius server host 147
radius server key 149
radius server msgauth 149
radius server primary 150
radius server retransmit 150
radius server timeout 151

radius source-interface 151
radius-auth-server 815
random-detect 1038
random-detect exponential weighting-constant 1038
random-detect queue-parms 1039
redirect 1055
redirect-url 816
redirect-url mode 815
redistribute (BGP Router Config) 879
redistribute (IPv6 Address Family Config) 880
redistribute (OSPF) 757
redistribute (OSPFv3) 980
redistribute (RIP) 801
release dhcp 670
reload (for chassis configuration) 30
reload (for stack configuration) 48
reload (Privileged EXEC) 231
remote-span 405
renew dhcp 671
renew dhcp network-port 671
renew dhcp service-port 671
rmon collection history 335
rmon event 334
rmon hcalarm 332
role priority 499
route-map 696
router bgp 839
router ospf 741
router rip 796
router-id (OSPF) 757
router-id (OSPFv3) 980
routing 667
save 303
script apply 166
script delete 166
script list 166
script show 166
script validate 167
script-text 820
sdm prefer 319
security 222
separator-color 822
serial baudrate 79
serial timeout 79
service dhcp 253

service dhcpv6 1010
service-policy 1060
serviceport ip 73
serviceport ipv6 address 923
serviceport ipv6 enable 923
serviceport ipv6 gateway 924
serviceport ipv6 neighbor 925
serviceport protocol 73
serviceport protocol dhcp 74
session start unit 301
session-limit 83
session-timeout (Captive Portal Instance) 818
session-timeout (Line Config) 83
set as-path 704
set clibanner 168
set comm-list delete 705
set community 705
set garp timer join 428
set garp timer leave 429
set garp timer leaveall 429
set gmrp adminmode 432
set gmrp interfacemode 433
set gvrp adminmode 430
set gvrp interfacemode 431
set igmp 549
set igmp fast-leave 550
set igmp groupmembership-interval 551
set igmp header-validation 554
set igmp interfacemode 550
set igmp maxresponse 552
set igmp mcrtrexpiretime 552
set igmp mrouter 553
set igmp mrouter interface 553
set igmp proxy-querier 562
set igmp querier 558
set igmp querier election participate 560
set igmp querier query-interval 559
set igmp querier timer expiry 559
set igmp querier version 560
set igmp report-suppression 554
set interface 706
set ip default next-hop 707
set ip next-hop 706
set ip precedence 708

set ipv6 next-hop (BGP) 708
set local-preference 709
set metric (BGP) 710
set mld 563
set mld fast-leave 564
set mld groupmembership-interval 565
set mld interfacemode 564
set mld maxresponse 566
set mld mcrtexpiretime 566
set mld mrouter 567
set mld mrouter interface 567
set mld proxy-querier 575
set mld querier 572
set mld querier election participate 573
set mld querier query_interval 572
set mld querier timer expiry 573
set prompt 167
set slot disable (for chassis configuration) 29
set slot disable (for stack configuration) 47
set slot power (for chassis configuration) 29
set slot power (for stack configuration) 48
set sup-console 80
sflow poller 314
sflow receiver 311
sflow receiver owner notimeout 312
sflow receiver owner timeout 312
sflow sampler 313
sflow source-interface 315
show “command” | begin “string” 176
show “command” | exclude “string” 175
show “command” | include “string” 175
show “command” | include “string” exclude “string2” 175
show “command” | section “string” 176
show “command” | section “string” “string2” 176
show “command” | section “string” include “string2” 177
show (Captive Portal Instance) 820
show (Privileged EXEC) 201
show aaa ias-users 131
show access-lists 1086
show access-lists vlan 1086
show accounting 132
show accounting methods 132
show arp 665
show arp access-list 541
show arp brief 666

show arp switch (Address Resolution Protocol commands) 666
show arp switch (system information and statistics commands) 178
show authentication authentication-history 445
show authentication interface 445
show authentication methods 447
show authentication statistics 448
show authorization methods 109
show auto-copy-sw (for chassis firmware synchronization) 39
show auto-copy-sw (for stack firmware synchronization) 63
show autoinstall 174
show auto-voip 1100
show auto-voip oui-table 1101
show backplane 37
show backplane-port 36
show backplane-port counters 36
show backplane-port diag 37
show backplane-port packet-path 37
show bgp ipv6 912
show bgp ipv6 aggregate-address 913
show bgp ipv6 community 913
show bgp ipv6 community-list 914
show bgp ipv6 neighbors 914
show bgp ipv6 neighbors advertised-routes 914
show bgp ipv6 neighbors policy 915
show bgp ipv6 route-reflection 915
show bgp ipv6 statistics 915
show bgp ipv6 summary 916
show bgp ipv6 update-group 916
show bootpdhcprelay 732
show bootvar 177
show captive-portal 811
show captive-portal client statistics 825
show captive-portal client status 824
show captive-portal configuration 822
show captive-portal configuration client status 826
show captive-portal configuration interface 823
show captive-portal configuration locales 824
show captive-portal configuration status 823
show captive-portal interface capability 828
show captive-portal interface client status 826
show captive-portal interface configuration status 827
show captive-portal status 811
show captive-portal trapflags 813
show captive-portal user 835

show capture packets 267
show chassis 31
show chassis watchdog 34
show chassis-status 35
show checkpoint statistics (for chassis configuration) 42
show checkpoint statistics (for stack configuration) 66
show class-map 1061
show classofservice dot1p-mapping 1040
show classofservice ip-dscp-mapping 1040
show classofservice ip-precedence-mapping 1041
show classofservice traffic-class-group 635
show classofservice trust 1041
show clibanner 168
show clock 244
show clock detail 244
show dampening interface 769
show debugging 292
show dhcp client vendor-id-option 524
show dhcp l2relay agent-option vlan 522
show dhcp l2relay all 520
show dhcp l2relay circuit-id vlan 520
show dhcp l2relay interface 521
show dhcp l2relay remote-id vlan 521
show dhcp l2relay stats interface 521
show dhcp l2relay subscription interface 522
show dhcp l2relay vlan 523
show dhcp lease 674
show diffserv 1062
show diffserv service 1065
show diffserv service brief 1066
show domain-name 133
show dos-control 605
show dot1q-tunnel 415
show dot1x 449
show dot1x authentication-history 454
show dot1x clients 454
show dot1x statistics 458
show dot1x users 455
show dvlan-tunnel 415
show eventlog 179
show exception 298
show fiber-ports optics 191
show fiber-ports optics-diag 192
show fiber-ports optics-eeprom 193
show fiber-ports optics-info 193

show fip-snooping 640
show fip-snooping enode 641
show fip-snooping fcf 643
show fip-snooping sessions 645
show fip-snooping statistics 649
show fip-snooping vlan 653
show flowcontrol 423
show forwardingdb agetime 607
show garp 430
show gmrp configuration 433
show green-mode 325
show green-mode eee-lpi-history 330
show gvrp configuration 431
show hardware 179
show hosts 262
show igmpsnooping 555
show igmpsnooping mrouter interface 556
show igmpsnooping mrouter vlan 557
show igmpsnooping proxy-querier 562
show igmpsnooping querier 560
show igmpsnooping ssm 557
show interface 181
show interface counters 183
show interface dampening 769
show interface debounce 621
show interface ethernet 185
show interface ethernet switchport 190
show interface lag 191
show interface loopback 932
show interface priority-flow-control 657
show interface tunnel 930
show interfaces cos-queue 1041
show interfaces random-detect 1042
show interfaces status 182
show interfaces switchport 411
show interfaces switchport (for a group ID) 426
show interfaces traffic 183
show ip access-lists 1084
show ip address-conflict 264
show ip arp inspection 538
show ip arp inspection interfaces 541
show ip arp inspection statistics 539
show ip as-path-access-list 920
show ip bgp 890

show ip bgp aggregate-address 893
show ip bgp community 894
show ip bgp community-list 894
show ip bgp neighbors 894
show ip bgp neighbors advertised-routes 899
show ip bgp neighbors policy 901
show ip bgp neighbors received-routes 901
show ip bgp route-reflection 902
show ip bgp statistics 903
show ip bgp summary 904
show ip bgp template 906
show ip bgp traffic 907
show ip bgp update-group 908
show ip brief 675
show ip community-list 920
show ip dhcp binding 255
show ip dhcp conflict 257
show ip dhcp global configuration 255
show ip dhcp pool configuration 256
show ip dhcp server statistics 256
show ip dhcp snooping 529
show ip dhcp snooping binding 530
show ip dhcp snooping database 531
show ip dhcp snooping interfaces 531
show ip dhcp snooping statistics 532
show ip dvmrp 1118
show ip dvmrp interface 1119
show ip dvmrp neighbor 1120
show ip dvmrp nexthop 1120
show ip dvmrp prune 1121
show ip dvmrp route 1121
show ip helper statistics 740
show ip helper-address 739
show ip http 101
show ip igmp 1141
show ip igmp groups 1142
show ip igmp interface 1143
show ip igmp interface membership 1144
show ip igmp interface stats 1145
show ip igmp-proxy 1146
show ip igmp-proxy groups 1148
show ip igmp-proxy groups detail 1149
show ip igmp-proxy interface 1147
show ip interface 676
show ip interface brief 678

show ip irdp 718
show ip mcast 1112
show ip mcast boundary 1112
show ip mcast interface 1113
show ip mcast mroute 1113
show ip mcast mroute group 1114
show ip mcast mroute source 1114
show ip mcast mroute static 1115
show ip ospf 775
show ip ospf abr 779
show ip ospf area 780
show ip ospf asbr 781
show ip ospf database 781
show ip ospf database database-summary 783
show ip ospf interface 783
show ip ospf interface brief 785
show ip ospf interface stats 786
show ip ospf lsa-group 788
show ip ospf neighbor 788
show ip ospf range 791
show ip ospf statistics 791
show ip ospf stub table 793
show ip ospf traffic 793
show ip ospf virtual-link 795
show ip ospf virtual-link brief 795
show ip pim 1130
show ip pim bsr-router 1134
show ip pim interface 1131
show ip pim neighbor 1133
show ip pim rp mapping 1136
show ip pim rp-hash 1135
show ip pim ssm 1131
show ip policy 710
show ip prefix-list 710
show ip protocols 679
show ip rip 802
show ip rip interface 803
show ip rip interface brief 802
show ip route 683
show ip route ecmp-groups 685
show ip route preferences 689
show ip route summary 686
show ip source binding 534
show ip ssh 88

show ip stats 690
show ip verify interface 534
show ip verify source 533
show ip vlan 721
show ip vrrp 729
show ip vrrp interface 729
show ip vrrp interface brief 731
show ip vrrp interface stats 728
show ipv6 access-lists 1093
show ipv6 brief 947
show ipv6 dhcp 1015
show ipv6 dhcp binding 1017
show ipv6 dhcp interface 1016
show ipv6 dhcp interface 951
show ipv6 dhcp pool 1018
show ipv6 dhcp snooping 1027
show ipv6 dhcp snooping binding 1028
show ipv6 dhcp snooping database 1029
show ipv6 dhcp snooping interfaces 1029
show ipv6 dhcp snooping statistics 1030
show ipv6 dhcp statistics 1016
show ipv6 interface 948
show ipv6 interface vlan 951
show ipv6 mld groups 1173
show ipv6 mld interface 1175
show ipv6 mld traffic 1177
show ipv6 mld-proxy 1179
show ipv6 mld-proxy groups 1180
show ipv6 mld-proxy groups detail 1181
show ipv6 mld-proxy interface 1180
show ipv6 mroute 1153
show ipv6 mroute group 1154
show ipv6 mroute source 1155
show ipv6 mroute static 1155
show ipv6 neighbors 952
show ipv6 ospf 993
show ipv6 ospf abr 996
show ipv6 ospf area 997
show ipv6 ospf asbr 998
show ipv6 ospf database 998
show ipv6 ospf database database-summary 999
show ipv6 ospf interface 1000
show ipv6 ospf interface brief 1001
show ipv6 ospf interface stats 1002
show ipv6 ospf lsa-group 1003

show ipv6 ospf max-metric 1005
show ipv6 ospf neighbor 1005
show ipv6 ospf range 1007
show ipv6 ospf statistics 1007
show ipv6 ospf stub table 1009
show ipv6 ospf virtual-link 1009
show ipv6 ospf virtual-link brief 1010
show ipv6 pim 1164
show ipv6 pim bsr-router 1168
show ipv6 pim interface 1165
show ipv6 pim neighbor 1167
show ipv6 pim rp mapping 1169
show ipv6 pim rp-hash 1169
show ipv6 pim ssm 1165
show ipv6 prefix-list 712
show ipv6 protocols 953
show ipv6 route 956
show ipv6 route ecmp-groups 958
show ipv6 route preferences 959
show ipv6 route summary 959
show ipv6 source binding 1032
show ipv6 traffic 962
show ipv6 verify 1031
show ipv6 verify source 1032
show ipv6 vlan 962
show iscsi 1106
show iscsi sessions 1107
show isdp 611
show isdp entry 613
show isdp interface 612
show isdp neighbors 614
show isdp traffic 615
show lacp actor 491
show lacp partner 492
show lldp 584
show lldp dcbx interface 627
show lldp interface 585
show lldp local-device 588
show lldp local-device detail 589
show lldp med 592
show lldp med interface 593
show lldp med local-device detail 594
show lldp med remote-device 595
show lldp med remote-device detail 596

show lldp remote-device 586
show lldp remote-device detail 587
show lldp statistics 585
show lldp tlv-select 627
show llpf interface 467
show logging 214
show logging buffered 215
show logging email config 220
show logging email statistics 221
show logging hosts 215
show logging persistent 216
show logging traplogs 216
show loginsession 102
show loginsession long 102
show mac access-lists 1072
show mac-address-table gmrp 434
show mac-address-table igmpsnooping 557
show mac-address-table mldsnooping 571
show mac-address-table multicast 608
show mac-address-table static 515
show mac-address-table staticfiltering 516
show mac-address-table stats 609
show mac-addr-table 195
show mail-server config 223
show management access-class 93
show management access-list 92
show mbuf 299
show mbuf total 300
show mldsnooping 568
show mldsnooping mrouter interface 569
show mldsnooping mrouter vlan 569
show mldsnooping proxy-querier 575
show mldsnooping querier 573
show mldsnooping ssm entries 569
show mldsnooping ssm groups 570
show mldsnooping ssm stats 570
show mmrp 471
show mmrp statistics 472
show monitor session 511
show mrp 469
show msg-queue 301
show mvr 546
show mvr interface 547
show mvr members 547
show mvr traffic 548

show mvrp 475
show mvrp statistics 475
show network 75
show network ipv6 dhcp statistics 1018
show network ipv6 neighbors 926
show nsf (for chassis configuration) 40
show nsf (for stack configuration) 65
show passwords configuration 125
show passwords result 126
show platform vpd 180
show poe 1190
show poe card 1192
show poe mpsm 1192
show poe port configuration 1193
show poe port info 1193
show policy-map 1062
show policy-map interface 1066
show port 360
show port advertise 362
show port description 363
show port protocol 403
show port-channel 493
show port-channel brief 492
show port-channel counters 494
show port-channel system priority 494
show port-security 578
show port-security dynamic 579
show port-security static 580
show port-security violation 580
show power redundancy 308
show power 308
show power matrix 308
show private-group 427
show process app-list 197
show process cpu 197
show process proc-list 198
show radius 152
show radius accounting 155
show radius accounting statistics 156
show radius servers 153
show radius source-interface 158
show radius statistics 158
show rmon 336
show rmon collection history 337

show rmon events 339
show rmon hcalarms 345
show rmon history 340
show rmon log 342
show rmon statistics interfaces 343
show route-map 714
show routing heap summary 690
show running-config 199
show running-config interface 200
show sdm prefer 319
show serial 80
show service-policy 1067
show serviceport 77
show serviceport ipv6 dhcp statistics 1020
show serviceport ipv6 neighbors 926
show sflow agent 315
show sflow pollers 316
show sflow receivers 316
show sflow samplers 318
show sflow source-interface 318
show slot 50
show snmpcommunity 143
show snmp-server 143
show snmptrap 144
show sntp 239
show sntp client 239
show sntp server 240
show sntp source-interface 241
show spanning-tree 380
show spanning-tree backbonefast 382
show spanning-tree brief 382
show spanning-tree interface 383
show spanning-tree mst detailed 385
show spanning-tree mst port detailed 387
show spanning-tree mst port summary 390
show spanning-tree mst port summary active 391
show spanning-tree mst summary 392
show spanning-tree summary 392
show spanning-tree uplinkfast 393
show spanning-tree vlan 394
show stack-port 55
show stack-port counters 55
show stack-port diag 56
show stack-port stack-path 61
show stack-status 50

show stats flow-based 353
show stats group 351
show storm-control 465
show supported cardtype (for chassis configuration) 30
show supported cardtype (for stack configuration) 51
show supported switchtype (for chassis configuration) 35
show supported switchtype (for stack configuration) 54
show sw reset 301
show switch 52
show switchport protected 425
show sysinfo 205
show tacacs 164
show tacacs source-interface 164
show tech-support 205
show telnet 85
show telnetcon 85
show terminal length 207
show time-range 1096
show trapflags 144
show udld 619
show usb device 310
show users 115
show users accounts 116
show users login-history [long] 117
show users login-history [username] 117
show users long 115
show version 179
show vlan 406
show vlan association mac 408
show vlan association subnet 408
show vlan internal usage 407
show vlan port 407
show vlan remote-span 512
show voice vlan 421
show vpc 502
show vpc brief 503
show vpc consistency-parameters 506
show vpc peer-keepalive 504
show vpc role 505
show vpc statistics 505
shutdown (Interface Config) 359
shutdown (Peer Template Config) 886
shutdown all 359
slot (for chassis configuration) 28

slot (for stack configuration) 46
snapshot bgp 303
snapshot multicast 304
snapshot ospf 303
snapshot routing 304
snapshot system 304
snmp trap link-status 142
snmp trap link-status all 142
snmp-server 134
snmp-server community 134
snmp-server community ipaddr 134
snmp-server community ipmask 135
snmp-server community mode 135
snmp-server community ro 136
snmp-server community rw 136
snmp-server enable traps 137
snmp-server enable traps bgp 139
snmp-server enable traps captive-portal 809
snmp-server enable traps linkmode 137
snmp-server enable traps multiusers 138
snmp-server enable traps stpmode 138
snmp-server enable traps violation 136
snmp-server port 139
snmptrap 139
snmptrap ipaddr 140
snmptrap mode 141
snmptrap snmpversion 140
snmptrap source-interface 141
sntp broadcast client poll-interval 236
sntp client mode 236
sntp client port 236
sntp server 238
sntp source-interface 238
sntp unicast client poll-interval 237
sntp unicast client poll-retry 237
sntp unicast client poll-timeout 237
spanning-tree 364
spanning-tree auto-edge 365
spanning-tree backbonefast 365
spanning-tree bpdufilter 366
spanning-tree bpdufilter default 367
spanning-tree bpduflood 367
spanning-tree bpduguard 367
spanning-tree bpdumigrationcheck 368
spanning-tree configuration name 368

spanning-tree configuration revision 369
spanning-tree cost 369
spanning-tree edgeport 369
spanning-tree forward-time 370
spanning-tree guard 370
spanning-tree max-age 371
spanning-tree max-hops 371
spanning-tree mode 371
spanning-tree mst 372
spanning-tree mst instance 373
spanning-tree mst priority 373
spanning-tree mst vlan 374
spanning-tree port mode 375
spanning-tree port mode all 375
spanning-tree port-priority 375
spanning-tree tcnguard 376
spanning-tree transmit 376
spanning-tree uplinkfast 376
spanning-tree vlan 377
spanning-tree vlan cost 377
spanning-tree vlan forward-time 378
spanning-tree vlan hello-time 378
spanning-tree vlan max-age 378
spanning-tree vlan port-priority 379
spanning-tree vlan priority 380
spanning-tree vlan root 379
speed 360
speed all 360
split-horizon 801
sshcon maxsessions 87
sshcon timeout 87
stack 44
stack-port 55
stack-status sample-mode 48
standby 46
stats flow-based (Global Config) 349
stats flow-based (Interface Config) 351
stats flow-based reporting 350
stats group (Global Config) 347
stats group (Interface Config) 350
storm-control broadcast 460
storm-control broadcast level 461
storm-control broadcast rate 461
storm-control multicast 462

storm-control multicast level 462
storm-control multicast rate 463
storm-control unicast 464
storm-control unicast level 464
storm-control unicast rate 465
sw reset 301
switch priority 44
switch renumber 45
switchport access vlan 410
switchport mode 408
switchport mode private-vlan 417
switchport private-group 426
switchport private-vlan 416
switchport protected (Global Config) 424
switchport protected (Interface Config) 425
switchport trunk allowed vlan 409
switchport trunk native vlan 410
system-mac 501
system-priority 500
tacacs-server host 160
tacacs-server key 160
tacacs-server keystring 161
tacacs-server source-interface 161
tacacs-server timeout 162
techsupport enable 303
telnet 81
telnetcon maxsessions 83
telnetcon timeout 84
telnetd 305
template peer 881
terminal length 206
timeout (TACACS Config) 164
time-range 1094
timers 887
timers bgp 888
timers pacing flood 759
timers pacing lsa-group (OSPF) 759
timers pacing lsa-group (OSPFv3) 980
timers spf 760
timers throttle spf 981
traceroute 223
track vpc interface 500
traffic-class-group max-bandwidth 632
traffic-class-group min-bandwidth 633
traffic-class-group strict 634

traffic-class-group weight 635
traffic-shape 1040
transport input telnet 82
transport output telnet 82
trapflags (Captive Portal Config Mode) 810
trapflags (OSPF) 760
trapflags (OSPFv3) 982
tunnel destination 930
tunnel mode ipv6ip 930
tunnel source 930
udld enable (Global Config) 617
udld enable (Interface Config) 618
udld message time 617
udld port 618
udld reset 618
udld timeout interval 618
update bootcode 178
update-source 887
user (Captive Portal Config Mode) 829
user group (captive portal local user commands) 831
user group (captive portal user group commands) 836
user group moveusers 837
user group name 837
user idle-timeout 832
user max-bandwidth-down 833
user max-bandwidth-up 832
user max-input-octets 833
user max-output-octets 834
user max-total-octets 834
user name (Captive Portal Config) 830
user password (Captive Portal Config) 830
user password encrypted 830
user session-timeout 831
user-logout 821
username (Global Config) 111
username (Mail Server Config) 222
username name nopassword 112
username name unlock 113
username snmpv3 accessmode 113
username snmpv3 authentication 113
username snmpv3 encryption 114
username snmpv3 encryption encrypted 115
verification 814
vlan 395

vlan acceptframe 396
vlan association mac 405
vlan association subnet 405
vlan database 395
vlan ingressfilter 396
vlan internal allocation 397
vlan makestatic 397
vlan name 398
vlan participation 398
vlan participation all 398
vlan port acceptframe all 399
vlan port ingressfilter all 400
vlan port priority all 422
vlan port pvid all 400
vlan port tagging all 400
vlan priority 422
vlan protocol group 401
vlan protocol group add protocol 401
vlan protocol group name 401
vlan pvid 404
vlan routing 719
vlan tagging 404
voice vlan (Global Config) 420
voice vlan (Interface Config) 420
voice vlan data priority 421
vpc 502
vpc domain 496
vpc peer-link 502
wip-msg 820
write core 297
write memory 235