



User Manual

**UM EN FL SWITCH GHS CLI for  
FL SWITCH GHS 12G/8  
FL SWITCH GHS 4G/12**

Gigabit Modular Switch

**Order No: -**



# AUTOMATION

## User Manual

Description of the CLI interface of the Gigabit Modular Switches

03/2017

---

Designation: UM EN FL SWITCH GHS CLI

Revision: 01

Order No: —

This user manual is valid for:

Designation	Revision	Order No:
FL SWITCH GHS 12G/8		2989200
FL SWITCH GHS 4G/12		2700271
FL FXT		2989307

## Please observe the following notes

In order to ensure the safe use of the product described, you have to read and understand this manual. The following notes provide information on how to use this manual.

### User group of this manual

The use of products described in this manual is oriented exclusively to qualified electricians or persons instructed by them, who are familiar with applicable standards and other regulations regarding electrical engineering and, in particular, the relevant safety concepts.

Phoenix Contact accepts no liability for erroneous handling or damage to products from Phoenix Contact or third-party products resulting from disregard of information contained in this manual.

### Explanation of symbols used and signal words



This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.



#### **DANGER**

This indicates a hazardous situation which, if not avoided, will result in death or serious injury.



#### **WARNING**

This indicates a hazardous situation which, if not avoided, could result in death or serious injury.



#### **CAUTION**

This indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

The following types of messages provide information about possible property damage and general information concerning proper operation and ease-of-use.



#### **NOTE**

This symbol and the accompanying text alerts the reader to a situation which may cause damage or malfunction to the device, either hardware or software, or surrounding property.



This symbol and the accompanying text provides additional information to the reader. It is also used as a reference to other sources of information (manuals, data sheets, literature) on the subject matter, product, etc.

---

### **General terms and conditions of use for technical documentation**

Phoenix Contact reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular data sheets, installation instructions, manuals, etc.) does not constitute any further duty on the part of Phoenix Contact to furnish information on alterations to products and/or technical documentation. Any other agreement shall only apply if expressly confirmed in writing by Phoenix Contact. Please note that the supplied documentation is product-specific documentation only and that you are responsible for checking the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. Although Phoenix Contact makes every effort to ensure that the information content is accurate, up-to-date, and state-of-the-art, technical inaccuracies and/or printing errors in the information cannot be ruled out. Phoenix Contact does not offer any guarantees as to the reliability, accuracy or completeness of the information. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed. This information does not include any guarantees regarding quality, does not describe any fair marketable quality, and does not make any claims as to quality guarantees or guarantees regarding the suitability for a special purpose.

Phoenix Contact accepts no liability or responsibility for errors or omissions in the content of the technical documentation (in particular data sheets, installation instructions, manuals, etc.).

The aforementioned limitations of liability and exemptions from liability do not apply, in so far as liability must be assumed, e.g., according to product liability law, in cases of premeditation, gross negligence, on account of loss of life, physical injury or damage to health or on account of the violation of important contractual obligations. Claims for damages for the violation of important contractual obligations are, however, limited to contract-typical, predictable damages, provided there is no premeditation or gross negligence, or that liability is assumed on account of loss of life, physical injury or damage to health. This ruling does not imply a change in the burden of proof to the detriment of the user.

### Statement of legal authority

This manual, including all illustrations contained herein, is copyright protected. Use of this manual by any third party is forbidden. Reproduction, translation, and public disclosure, as well as electronic and photographic archiving or alteration requires the express written consent of Phoenix Contact. Violators are liable for damages.

Phoenix Contact reserves all rights in the case of patent award or listing of a registered design. Third-party products are always named without reference to patent rights. The existence of such rights shall not be excluded.

### How to contact us

#### Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:

[www.phoenixcontact.com](http://www.phoenixcontact.com).

Make sure you always use the latest documentation.

It can be downloaded at:

[www.phoenixcontact.net/catalog](http://www.phoenixcontact.net/catalog).

#### Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary.

Subsidiary contact information is available at [www.phoenixcontact.com](http://www.phoenixcontact.com).

#### Published by

PHOENIX CONTACT GmbH & Co. KG

Flachsmarktstraße 8

32825 Blomberg

Germany

Phone +49 - (0) 52 35 - 3-00

Fax +49 - (0) 52 35 - 3-4 12 00

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send your comments to

[tecdoc@phoenixcontact.com](mailto:tecdoc@phoenixcontact.com).



- exit-overflow-interval (OSPF) ..... 10
- external-lsdb-limit (OSPF) ..... 11
- router-id (OSPF) ..... 11
- redistribute (OSPF) ..... 11
- maximum-paths (OSPF) ..... 12
- passive-interface default (OSPF) ..... 12
- passive-interface (OSPF) ..... 12
- trapflags (OSPF) ..... 13
- show ip ospf ..... 15
- Note: show ip ospf ..... 16
- show ip ospf area ..... 20
- show ip ospf asbr ..... 21
- show ip ospf database ..... 21
- show ip ospf database database-summary ..... 22
- show ip ospf interface ..... 23
- show ip ospf interface brief ..... 24
- show ip ospf interface stats ..... 24
- Table 10:show ip ospf neighbor ..... 26
- Example:show ip ospf range ..... 27
- show ip ospf statistics ..... 28
- show ip ospf stub table ..... 28
- show ip ospf virtual-link ..... 29
- show ip ospf virtual-link brief ..... 29
  
- Display ..... 30
  
- Port Configuration Commands ..... 30
  - interface ..... 30
  
- Basic Port Features ..... 30
  
- auto-negotiate ..... 31
  - Note: auto-negotiate all ..... 31
  - Note: description ..... 32
  - Note: mtu ..... 32
  - Note: shutdown ..... 32
  - Note: speed all ..... 33
  - Note: show port ..... 33
  
- Spanning Tree Protocol (STP) Commands ..... 34
  - Note: spanning-tree ..... 34
  - Note: spanning-tree bpdupfilter ..... 34
  - Note: spanning-tree bpdupfilter default ..... 35
  - Note: spanning-tree bpdupflood ..... 35
  - Note: spanning-tree bpduguard ..... 35

---

Note:	spanning-tree bpdumigrationcheck .....	36
Note:	spanning-tree configuration name .....	36
Note:	spanning-tree configuration revision .....	36
Note:	spanning-tree edgeport .....	37
Note:	spanning-tree forceversion .....	37
•	spanning-tree forward-time .....	38
•	spanning-tree hello-time .....	38
•	spanning-tree max-age .....	38
•	spanning-tree max-hops .....	39
•	spanning-tree mst .....	39
•	spanning-tree mst instance .....	40
•	spanning-tree mst priority .....	41
•	spanning-tree mst vlan .....	41
•	spanning-tree port mode .....	42
•	spanning-tree port mode all .....	42
•	show spanning-tree .....	42
•	show spanning-tree brief .....	43
•	show spanning-tree interface .....	44
•	show spanning-tree mst port detailed .....	44
•	show spanning-tree mst port summary .....	46
•	show spanning-tree mst summary .....	46
•	show spanning-tree summary .....	47
•	show spanning-tree vlan .....	47
•	<b>VLAN Commands .....</b>	<b>48</b>
•	vlan database .....	48
•	network mgmt_vlan .....	48
•	vlan .....	48
•	vlan acceptframe .....	49
•	vlan ingressfilter .....	49
•	vlan makestatic .....	50
•	vlan name .....	50
•	vlan participation .....	50
•	vlan participation all .....	51
•	vlan port acceptframe all .....	51
•	vlan port ingressfilter all .....	52
•	vlan port pvid all .....	52
•	vlan port tagging all .....	52
•	vlan pvid .....	53
•	vlan tagging .....	53
•	vlan tagging mode .....	53
•	show vlan mode .....	54
•	show vlan .....	54
•	show vlan brief .....	55
•	show vlan port .....	55

## Product designation

---

•	Provisioning (IEEE 802.1p) Commands .....	56
	•	vlan port priority all ..... 56
	•	vlan priority ..... 56
•	GARP Commands .....	56
	•	show garp ..... 56
•	GVRP Commands .....	57
	Note:	set gvrp adminmode ..... 57
	Note:	set gvrp interfacemode ..... 57
	•	show gvrp configuration ..... 58
•	GMRP Commands .....	58
	Note:	set gmrp adminmode ..... 58
	Note:	set gmrp interfacemode ..... 59
	•	show gmrp configuration ..... 59
•	Port-Based Network Access Control Commands .....	60
	•	clear dot1x statistics ..... 60
	•	clear radius statistics ..... 60
	•	dot1x guest-vlan ..... 60
	•	dot1x max-req ..... 61
	•	dot1x port-control ..... 61
	•	dot1x re-authenticate ..... 62
	•	dot1x re-authentication ..... 62
	•	dot1x system-auth-control ..... 62
	•	dot1x timeout ..... 63
	•	show dot1x ..... 64
•	Storm-Control Commands .....	66
	•	storm-control broadcast ..... 66
	•	storm-control broadcast all ..... 66
	•	storm-control multicast ..... 67
	•	storm-control multicast rate ..... 67
	•	storm-control multicast all ..... 68
	•	storm-control multicast all rate ..... 68
	•	storm-control unicast ..... 68
	•	storm-control unicast rate ..... 69
	•	storm-control unicast all ..... 69
	•	storm-control unicast all rate ..... 70
	•	storm-control flowcontrol ..... 70
	Note:	show storm-control ..... 71

---

Note: Port-Channel/LAG (802.3ad) Commands .....	71
Note: port-channel .....	72
Note: addport .....	72
Note: deleteport (Interface Config) .....	72
Note: deleteport (Global Config) .....	73
Note: lacp admin key .....	73
Note: lacp collector max-delay .....	73
Note: lacp actor admin .....	74
Note: lacp actor admin key .....	74
Note: lacp actor admin state .....	74
Note: lacp actor admin state individual .....	75
Note: lacp actor admin state longtimeout .....	75
Note: lacp actor admin state passive .....	76
Note: lacp actor port .....	76
Note: lacp actor port priority .....	76
Note: lacp actor system priority .....	76
Note: lacp partner admin key .....	77
Note: lacp partner admin state .....	77
Note: lacp partner admin state individual .....	78
Note: lacp partner admin state longtimeout .....	78
Note: lacp partner admin state passive .....	79
Note: lacp partner port id .....	79
Note: lacp partner port priority .....	79
Note: lacp partner system-id .....	80
Note: lacp partner system priority .....	80
Note: port-channel static .....	81
Note: port lacpmode .....	81
Note: port lacpmode enable all .....	82
Note: port lacptimeout (Interface Config) .....	82
Note: port lacptimeout (Global Config) .....	82
Note: port-channel adminmode .....	83
Note: port-channel linktrap .....	83
Note: port-channel name .....	84
Note: port-channel system priority .....	84
Note: show lacp actor .....	84
Note: show lacp partner .....	84
Note: show port-channel brief .....	85
• show port-channel .....	85
• show port-channel system priority .....	86
• Port Mirroring .....	86
• monitor session .....	86
Note: no monitor .....	87
Note: show monitor session .....	87

Note: IGMP Snooping Configuration Commands ..... 88

- Note: set igmp ..... 88
  - show igmpsnooping ..... 89
  - show igmpsnooping mrouter interface ..... 90
  - show igmpsnooping mrouter vlan ..... 91
- IGMP Snooping Querier Commands ..... 91
  - set igmp querier ..... 91
  - set igmp querier query-interval ..... 92
  - set igmp querier version ..... 92
  - garp ..... Configure Generic Attribute Registration Protocol parameters .....  
gmrpSet GARP Multicast Registration parameters  
gvrpSet GARP VLAN Registration Protocol parameters  
igmpEnable/Disable IGMP Snooping parameters ..... 93
  - (Broadcom FASTPATH Switching) (Config)#set igmp? <cr> ..... Press enter to execute the command 93
  - show igmpsnooping ..... 94
  - show igmpsnooping mrouter interface ..... 95
  - show igmpsnooping mrouter vlan ..... 95
- Port Security Commands ..... 95
  - Note: port-security ..... 96
    - port-security max-dynamic ..... 96
    - port-security max-static ..... 97
    - port-security mac-address ..... 97
    - port-security mac-address move ..... 97
    - show port-security ..... 97
    - show port-security dynamic ..... 98
    - show port-security static ..... 98
    - show port-security violation ..... 98
- LLDP (802.1AB) Commands ..... 99
  - lldp transmit ..... 99
  - lldp receive ..... 99
  - lldp timers ..... 99
  - lldp transmit-tlv ..... 100
  - lldp transmit-mgmt ..... 100
  - lldp notification ..... 101
  - clear lldp statistics ..... 101
  - clear lldp remote-data ..... 101
  - show lldp ..... 101
  - show lldp interface ..... 102
  - show lldp statistics ..... 102
  - show lldp remote-device ..... 103
  - show lldp remote-device detail ..... 103

---

•	show lldp local-device .....	104
•	show lldp local-device detail .....	104
•	LLDP-MED Commands .....	105
•	lldp med .....	105
•	lldp med confignotification .....	105
•	lldp med transmit-tlv .....	106
•	show lldp med .....	106
	Example:show lldp med interface .....	107
	Example:show lldp med local-device detail .....	108
	Example:show lldp med remote-device .....	109
	Example:show lldp med remote-device detail .....	109
	Example: MAC Database Commands .....	110
	Example:bridge aging-time .....	111
	Example:show forwardingdb agetime .....	111
	..... Static Mcast Configuration	1
	Static_mcast create .....	1
	Static_mcast delete .....	1
	add_port .....	1
	rem_port .....	1
	Set IGMP.....	1
	block-unknown-mcast .....	1
	forward-unknown-mcast .....	1
•	Class of Service (CoS) Commands .....	1
Note:	classofservice dot1p-mapping .....	1
•	classofservice ip-dscp-mapping .....	1
•	cos-queue strict .....	3
•	traffic-shape .....	3
•	show classofservice dot1p-mapping .....	4
•	show classofservice ip-dscp-mapping .....	4
•	show interfaces cos-queue .....	4
•	MAC Access Control List (ACL) Commands .....	5
•	mac access-list extended .....	5
Note:	mac access-list extended rename .....	6
Note:	{deny   permit} .....	6
Note:	mac access-group .....	8
•	show mac access-lists .....	8
•	IP Access Control List (ACL) Commands .....	9
•	access-list .....	9

	Note: ip access-group .....	11
	• acl-trapflags .....	11
	• show ip access-lists .....	12
	Note: show access-lists .....	12
•	Dual Image Commands .....	1
	• delete .....	1
	• boot system .....	1
	• show bootvar .....	1
	• filedescr .....	2
	• update bootcode .....	2
•	System Information and Statistics Commands .....	2
	• show arp switch .....	2
	• show hardware .....	2
	Note: show version .....	3
	Note: show interface .....	3
	Note: show interface ethernet .....	4
	• show mac-addr-table .....	10
	• show running-config .....	11
	• show sysinfo .....	12
	• show tech-support .....	13
	• terminal length .....	13
	• show terminal length .....	14
•	Logging Commands .....	14
	• show logging buffered .....	14
•	System Utility and Clear Commands .....	14
	• traceroute .....	14
	Example:clear config .....	16
	Example:clear counters .....	16
	Example:clear igmpsnooping .....	16
	Example:clear pass .....	16
	Example:clear port-channel .....	16
	Example:clear traplog .....	16
	Example:clear vlan .....	17
	Example:enable passwd .....	17
	Example:enable passwd encrypted <password> .....	17
	Example:logout .....	17
	• ping .....	17
	Example:quit .....	19
	• reload .....	19
	• copy .....	19

---

Table 13: Simple Network Time Protocol (SNTP) Commands .....	21
Table 13:sntp broadcast client poll-interval .....	21
Table 13:sntp client mode .....	21
Table 13:sntp client port .....	21
Table 13:sntp unicast client poll-interval .....	22
Table 13:sntp unicast client poll-timeout .....	22
Table 13:sntp unicast client poll-retry .....	22
Table 13:sntp multicast client poll-interval .....	23
Table 13:sntp server .....	23
Table 13:show sntp .....	23
Table 13:show sntp client .....	24
Table 13:show sntp server .....	24
Section 5: Network Interface Commands .....	1
• enable (Privileged EXEC access) .....	1
• network parms .....	1
• network protocol .....	1
• network mac-address .....	2
• network mac-type .....	2
• network javamode .....	2
• show network .....	3
Example: Console Port Access Commands .....	3
Example:configure .....	4
Example:lineconfig .....	4
Example:serial baudrate .....	4
Example:serial timeout .....	4
Example:show serial .....	5
• Telnet Commands .....	5
• ip telnet server enable .....	5
• telnet .....	6
• transport input telnet .....	6
Note: transport output telnet .....	6
Note: session-limit .....	7
Note: session-timeout .....	7
Note: telnetcon maxsessions .....	8
Note: telnetcon timeout .....	8
Note: show telnet .....	9
• show telnetcon .....	9
• Secure Shell (SSH) Commands .....	9
Note: ip ssh .....	10
Note: ip ssh protocol .....	10
Note: ip ssh server enable .....	10

## Product designation

---

Note: sshcon maxsessions .....	10
Note: sshcon timeout .....	11
Note: show ip ssh .....	11
Note: Management Security Commands .....	12
Note: Hypertext Transfer Protocol (HTTP) Commands .....	12
Note: ip http server .....	12
Note: ip http secure-server .....	12
Note: ip http java .....	13
Note: ip http session hard-timeout .....	13
Note: ip http session maxsessions .....	14
Note: ip http session soft-timeout .....	14
Note: ip http secure-session hard-timeout .....	14
Note: ip http secure-session maxsessions .....	15
Note: ip http secure-session soft-timeout .....	15
Note: ip http secure-port .....	15
Note: ip http secure-protocol .....	16
Note: show ip http .....	16
Note: Access Commands .....	17
Note: disconnect .....	17
Note: show loginsession .....	17
Note: User Account Commands .....	18
Note: users name .....	18
Note: users passwd .....	18
Note: users passwd <username> encrypted <password> .....	19
Note: show users .....	19
Note: show users accounts .....	20
Note: passwords min-length .....	20
Note: passwords history .....	20
Note: passwords aging .....	21
Note: passwords lock-out .....	21
Note: write memory .....	22
Note: Configuration .....	22
Note: show memcard .....	22
Note: Show Commands in Privileged Exec Mode for SFP, POE, SCRJ, Temperature, DHCP Relay Agent, enhanced Port Information and Time: 22	
Note: Config Commands in Privileged Exec Mode for time settings at Real Time Clock: .....	23
Note: Config Commands in Global Config Mode for SNTP and DHCP Relay Agent: .....	23

---

Note: Config Commands for POE and DHCP Relay Agent in Interface Config Mode: .....	23
Note: MRP Commands .....	24
Note: Spanning Tree enhanced Commands: .....	25
Note: PROFINET .....	26
• Profinet Commands .....	26
• Digital Input CLI commands .....	26
• Link Monitoring CLI commands .....	26
• Alarm contact CLI commands .....	27
• SNMP Commands .....	27
• snmp-server .....	27
• snmp-server community .....	28
• snmp-server community ipaddr .....	28
• snmp-server community ipmask .....	28
• snmp-server community mode .....	29
• snmp-server community ro .....	29
• snmp-server community rw .....	30
• snmp-server enable traps violation .....	30
Note: snmp-server enable traps .....	30
Note: snmptrap .....	31
Note: snmptrap ipaddr .....	32
Note: show snmpcommunity .....	32
Note: show snmptrap .....	32
Example:show trapflags .....	33
Example: RADIUS Commands .....	34
Example:authorization network radius .....	34
Example:radius accounting mode .....	34
Example:radius server attribute 4 .....	34
Example:radius server host .....	35
Note: radius server key .....	36
Example:radius server msgauth .....	36
Example:radius server primary .....	37
Example:radius server retransmit .....	37
Example:radius server timeout .....	37
Example:show radius .....	38
Example:show radius accounting .....	38
Example:show radius statistics .....	39
Example: Routing Commands .....	40
Example:VRRP .....	40
Example: VRRP Virtual Router Redundancy Protocol Commands .....	40
Example:ip vrrp (Global Config) .....	41

- Example:ip vrrp (Interface Config) ..... 41
- Example:ip vrrp mode ..... 41
- Example:ip vrrp ip ..... 42
- Example:ip vrrp authentication ..... 42
- Example:ip vrrp preempt ..... 43
- Example:ip vrrp priority ..... 43
- Example:ip vrrp timers advertise ..... 44
- Example:show ip vrrp interface stats ..... 44
  - show ip vrrp ..... 45
  - show ip vrrp interface ..... 45
  - show ip vrrp interface brief ..... 46
- OSPF ..... 46
  - bandwidth ..... 47
  - ip ospf authentication ..... 47
  - ip ospf cost ..... 48
  - ip ospf dead-interval ..... 48
  - Note: ip ospf hello-interval ..... 48
  - Note: ip ospf network ..... 49
  - Note: ip ospf priority ..... 49
  - Note: ip ospf retransmit-interval ..... 50
  - Note: ip ospf transmit-delay ..... 50
  - Note: router ospf ..... 51
  - Note: enable (OSPF) ..... 51
  - Note: network area (OSPF) ..... 51
- Note: IP Routing Commands ..... 52
  - Note: routing ..... 52
  - Note: ip routing ..... 52
  - Note: ip address ..... 53
  - Note: ip route ..... 53
    - ip route default ..... 54
    - ip route distance ..... 54
    - ip netdirbcast ..... 55
    - ip mtu ..... 55
  - Note: encapsulation ..... 56
  - Note: show ip brief ..... 56
    - show ip interface ..... 57
    - show ip route ..... 59
  - Example:show ip route summary ..... 60
  - Example:show ip route preferences ..... 61
    - show ip stats ..... 62
- Routing Information Protocol (RIP) Commands ..... 62
  - router rip ..... 62
  - enable (RIP) ..... 62

---

•	ip rip .....	62
•	auto-summary .....	63
•	default-information originate (RIP) .....	63
•	default-metric (RIP) .....	63
•	distance rip .....	64
•	distribute-list out (RIP) .....	64
•	ip rip authentication .....	64
•	ip rip receive version .....	65
•	ip rip send version .....	65
•	hostroutesaccept .....	66
•	split-horizon .....	66
•	redistribute (RIP) .....	66
•	show ip rip .....	67
•	show ip rip interface brief .....	68
•	show ip rip interface .....	68
•	Configuration Scripting Commands .....	69
	Note: script apply .....	70
	Note: script delete .....	70
	Note: script list .....	70
	Note: script show .....	70
	Note: script validate .....	71
	Note: .....	71



# Section 1: Using the Command-Line Interface

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

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

- [“Command Syntax” on page 1](#)
- [“Command Conventions” on page 2](#)
- [“Common Parameter Values” on page 2](#)
- [“Slot/Port Naming Convention” on page 3](#)
- [“Using the “No” Form of a Command” on page 4](#)
- [“Command Modes” on page 4](#)
- [“Command Modes” on page 4](#)
- [“Command Completion and Abbreviation” on page 6](#)
- [“CLI Error Messages” on page 7](#)
- [“CLI Line-Editing Conventions” on page 7](#)
- [“Using CLI Help” on page 8](#)
- [“Accessing the CLI” on page 9](#)

## 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` or `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 parameter, so you are not required to enter a value in place of the parameter.

The *CLI Command Reference* 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

In this document, the command name is in **bold** font. Parameters are in *italic font*. You must replace the parameter name with an appropriate value, which might be a name or number. Parameters are order dependent.

The parameters for a command might include mandatory values, optional values, or keyword choices. [Table 1](#) describes the conventions this document uses to distinguish between value types.

**Table 1: Parameter Conventions**

Symbol	Example	Description
<> angle brackets	<i>&lt;value&gt;</i>	Indicates that you must enter a value in place of the brackets and text inside them.
[] square brackets	<i>[value]</i>	Indicates an optional parameter that you can enter in place of the brackets and text inside them.
{ } curly braces	<i>{choice1   choice2}</i>	Indicates that you must select a parameter from the list of choices.
Vertical bars	<i>choice1   choice2</i>	Separates the mutually exclusive choices.
[{ } Braces within square brackets	<i>[{choice1   choice2}]</i>	Indicates a choice within an optional element.

## 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. [Table 2](#) describes common parameter values and value formatting.

Table 2: Parameter Descriptions

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

## SLOT/PORT NAMING CONVENTION

FL SWITCH GHS Firmware software references physical entities such as cards and ports by using a slot/port naming convention. The FL SWITCH GHS Firmware 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.
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 zero.

**Table 4: Type of Ports**

Port Type	Description
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 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 re-enable a disabled feature or to enable a feature that is disabled by default. Only the configuration commands are available in the `no` form.

## COMMAND MODES

The CLI groups commands into modes according to the command function. Each of the command modes supports specific FL SWITCH GHS Firmware 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. [Table 5](#) 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 RIP does not have the Router RIP Command Mode.

**Table 5: CLI Command Modes**

Command Mode	Prompt	Mode Description
User EXEC	<code>switch&gt;</code>	Contains a limited set of commands to view basic system information.
Privileged EXEC	<code>switch#</code>	Allows you to issue any <code>EXEC</code> command, enter the VLAN mode, or enter the Global Configuration mode.

Table 5: CLI Command Modes (Cont.)

Command Mode	Prompt	Mode Description
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 <slot/port>)#	Manages the operation of an interface and provides access to the router interface configuration commands.
	Switch (Interface Loopback <id>)#	Use this mode to set up a physical port for a specific logical connection operation.
	Switch (Interface Tunnel <id>)#	
Line Config	Switch (line)#	Contains commands to configure outbound telnet settings and console interface settings.
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.
Router OSPF Config	Switch (Config-router)#	Contains the OSPF configuration commands.
Router RIP Config	Switch (Config-router)#	Contains the RIP 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.
DHCP Pool Config	Switch (Config dhcp-pool)#	Contains the DHCP server IP address pool configuration commands.

Table 6 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 <code>logout</code> .
Privileged EXEC	From the User EXEC mode, enter <code>enable</code> .	To exit to the User EXEC mode, enter <code>exit</code> or press <code>Ctrl-Z</code> .
Global Config	From the Privileged EXEC mode, enter <code>configure</code> .	To exit to the Privileged EXEC mode, enter <code>exit</code> , or press <code>Ctrl-Z</code> .
VLAN Config	From the Privileged EXEC mode, enter <code>vlan database</code> .	To exit to the Privileged EXEC mode, enter <code>exit</code> , or press <code>Ctrl-Z</code> .
Interface Config	From the Global Config mode, enter <code>interface &lt;slot/port&gt;</code> or <code>interface loopback &lt;id&gt;</code> or <code>interface tunnel &lt;id&gt;</code>	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .
Line Config	From the Global Config mode, enter <code>lineconfig</code> .	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .
Policy-Map Config	From the Global Config mode, enter <code>policy-map</code> .	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .

Table 6: CLI Mode Access and Exit (Cont.)

Command Mode	Access Method	Exit or Access Previous Mode
Policy-Class-Map Config	From the Policy Map mode enter <code>class</code> .	To exit to the Policy Map mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .
Class-Map Config	From the Global Config mode, enter <code>class-map</code> , and specify the optional keyword <code>ipv4</code> to specify the Layer 3 protocol for this class. See “ <a href="#">class-map</a> ” on <a href="#">page 8</a> for more information.	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .
Router OSPF Config	From the Global Config mode, enter <code>router ospf</code> .	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .
Router RIP Config	From the Global Config mode, enter <code>router rip</code> .	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .
MAC Access-list Config	From the Global Config mode, enter <code>mac access-list extended &lt;name&gt;</code> .	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .

## 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. [Table 7](#) 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

[Table 8](#) 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

**Table 8: CLI Editing Conventions (Cont.)**

Key Sequence	Description
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.

```
(switch) >?
```

```
enable          Enter into user privilege mode.
help            Display help for various special keys.
logout          Exit this session. Any unsaved changes are lost.
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.

```
(switch) #network ?
```

```
javamode        Enable/Disable.
mgmt_vlan       Configure the Management VLAN ID of the switch.
parms           Configure Network Parameters of the router.
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.

```
(switch) #network parms ?
```

```
<ipaddr>        Enter the IP address.
```

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:

```
(switch) #show m?
```

```
mac-addr-table   mac-address-table   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 1](#).



## Section 2: Switching Commands

This chapter describes the switching commands available in the FL SWITCH GHS Firmware CLI.



**Caution!** 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.

### 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. You must specify the area ID and an integer value between 1-16777215.

**Format**            area <areaid> default-cost <1-16777215>  
**Mode**              Router OSPF Config

### area nssa (OSPF)

This command configures the specified areaid to function as an NSSA.

**Format**            area <areaid> nssa  
**Mode**              Router OSPF Config

*no area nssa*

This command disables nssa from the specified area id.

**Format**        **no area <areaid> 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 is to be in a range of 1-16777214. If no metric is specified, the default value is \*\*\*\*. The metric type can be comparable (nssa-external 1) or non-comparable (nssa-external 2).

**Format**        **area <areaid> 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 <areaid> 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 <areaid> 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 <areaid> 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 <areaid> nssa no-summary`

**Mode**             Router OSPF Config

*no area nssa no-summary (OSPF)*

This command disables nssa from the summary LSAs.

**Format**            `no area <areaid> nssa no-summary`

**Mode**             Router OSPF Config

**area nssa translator-role (OSPF)**

This command configures the translator role of the NSSA. A value of *always* causes the router to assume the role of the translator the instant it becomes a border router and a value of *candidate* causes the router to participate in the translator election process when it attains border router status.

**Format**            `area <areaid> 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 <areaid> 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 <areaid> 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 <areaid> nssa translator-stab-intv <stabilityinterval>`

**Mode** Router OSPF Config

**area range (OSPF)**

This command creates a specified area range for a specified NSSA. The *<ipaddr>* is a valid IP address. The *<subnetmask>* is a valid subnet mask. The LSDB type must be specified by either **summarylink** or **nssaexternallink**, and the advertising of the area range can be allowed or suppressed.

**Format** `area <areaid> range <ipaddr> <subnetmask> {summarylink | nssaexternallink} [advertise | not-advertise]`

**Mode** Router OSPF Config

*no area range*

This command deletes a specified area range. The *<ipaddr>* is a valid IP address. The *<subnetmask>* is a valid subnet mask.

**Format** `no area <areaid> range <ipaddr> <subnetmask>`

**Mode** Router OSPF Config

**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 <areaid> stub`

**Mode** Router OSPF Config

*no area stub*

This command deletes a stub area for the specified area ID.

**Format** `no area <areaid> stub`

**Mode** Router OSPF Config

**area stub no-summary (OSPF)**

This command configures the Summary LSA mode for the stub area identified by *<areaid>*. Use this command to prevent LSA Summaries from being sent.

**Default** disabled

**Format** `area <areaid> 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 *<areaid>*.

**Format** `no area <areaid> stub no-summary`

**Mode** Router OSPF Config

**area virtual-link (OSPF)**

This command creates the OSPF virtual interface for the specified *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor.

**Format** `area <areaid> virtual-link <neighbor>`

**Mode** Router OSPF Config

*no area virtual-link*

This command deletes the OSPF virtual interface from the given interface, identified by *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor.

**Format** `no area <areaid> 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 *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor. The value for *<type>* is either none, simple, or encrypt. The *[key]* is composed of standard displayable, non-control 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 may be up to 16 bytes. Unauthenticated interfaces do not need an authentication key. If the type is encrypt, a key id 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 <areaid> 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 *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor.

**Format** `no area <areaid> 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 *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor. The range for seconds is 1 to 65535.

**Default** 40

**Format** `area <areaid> 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 *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor.

**Format** `no area <areaid> 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 *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor. The range for *<seconds>* is 1 to 65535.

**Default** 10

**Format** `area <areaid> 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 *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor.

**Format** `no area <areaid> 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 *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor. The range for seconds is 0 to 3600.

**Default** 5

**Format** `area <areaid> 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 <areaid> and <neighbor>. The <neighbor> parameter is the Router ID of the neighbor.

**Format** `no area <areaid> 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 <areaid> 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 <areaid> 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 <areaid> 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`), 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` command to change the reference bandwidth, specifying the reference bandwidth in megabits per second (Mbps). The reference bandwidth range is 1-4294967 Mbps. The different reference bandwidth can be independently configured for OSPFv2 and OSPFv3.

**Default** 100Mbps

**Format** `auto-cost reference-bandwidth <1 to 4294967>`  
**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

### **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. 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.

**Default** actual interface bandwidth  
**Format** `bandwidth <1-10000000>`  
**Mode** Interface Config

*no bandwidth*

Use this command to set the interface bandwidth to its default value.

**Format** `no bandwidth`  
**Mode** Interface 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. FL SWITCH GHS Firmware supports the storing and flooding of Opaque LSAs of different scopes.

**Default** disabled  
**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

**default-information originate (OSPF)**

This command is used to control the advertisement of default routes.

**Default**

- metric—unspecified
- type—2

**Format** `default-information originate [always] [metric <0-16777214>] [metric-type {1 | 2}]`

**Mode** Router OSPF Config

*no default-information originate (OSPF)*

This command is used to control the advertisement of default routes.

**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.

**Format** `default-metric <1-16777214>`

**Mode** Router OSPF Config

*no default-metric (OSPF)*

This command is used to set a 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*, *inter*, 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 <1-255> | inter-area <1-255> | external <1-255>}`

**Mode** Router OSPF Config

*no distance ospf*

This command sets the default route preference value of OSPF routes in the router. The type of OSPF 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 OSPF Config

### **distribute-list out (OSPF)**

Use this command to specify the access list to filter routes received from the source protocol.

**Format** `distribute-list <1-199> out {rip | bgp | static | connected}`

**Mode** Router OSPF Config

*no distribute-list out*

Use this command to specify the access list to filter routes received from the source protocol.

**Format** `no distribute-list <1-199> 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 non-default AS-external-LSAs. When set to 0, the router will not leave overflow state until restarted. The range for seconds 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 non-default 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 non-default AS-external-LSAs in its database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area. The range for limit is -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

**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 OSPF protocol to allow redistribution of routes from the specified source protocol/routers.

**Default**

- metric—unspecified
- type—2
- tag—0

**Format** `redistribute {rip | bgp | static | connected} [metric <0-16777214>] [metric-type {1 | 2}] [tag <0-4294967295>] [subnets]`  
**Mode** Router OSPF Config

*no redistribute*

This command configures OSPF protocol to prohibit redistribution of routes from the specified source protocol/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 where *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 (OSPF)**

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 non-passive mode.

**Format** `no passive-interface default`

**Mode** Router OSPF Config

### **passive-interface (OSPF)**

Use this command to set the interface or tunnel as passive. It overrides the global passive mode that is currently effective on the interface or tunnel.

**Default** disabled

**Format** `passive-interface {<slot/port> | tunnel <tunnel-id>}`

**Mode** Router OSPF Config

*no passive-interface*

Use this command to set the interface or tunnel as non-passive. It overrides the global passive mode that is currently effective on the interface or tunnel.

**Format** `no passive-interface {<slot/port> | tunnel <tunnel-id>}`

**Mode** Router OSPF Config

*timers spf*

Use this command to configure the SPF delay time and hold time. The valid range for both 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 [Table 9](#).

**Table 9: Trapflags Groups**

Group	Flags
<b>errors</b>	<ul style="list-style-type: none"> <li>• authentication-failure</li> <li>• bad-packet</li> <li>• config-error</li> <li>• virt-authentication-failure</li> <li>• virt-bad-packet</li> <li>• virt-config-error</li> </ul>
<b>if-rx</b>	ir-rx-packet
<b>lsa</b>	<ul style="list-style-type: none"> <li>• lsa-maxage</li> <li>• lsa-originate</li> </ul>
<b>overflow</b>	<ul style="list-style-type: none"> <li>• lsdb-overflow</li> <li>• lsdb-approaching-overflow</li> </ul>
<b>retransmit</b>	<ul style="list-style-type: none"> <li>• packets</li> <li>• virt-packets</li> </ul>
<b>rtb</b>	<ul style="list-style-type: none"> <li>• rtb-entry-info</li> </ul>
<b>state-change</b>	<ul style="list-style-type: none"> <li>• if-state-change</li> <li>• neighbor-state-change</li> <li>• virtif-state-change</li> <li>• virtneighbor-state-change</li> </ul>

- To enable the individual flag, enter the **group name** followed by that particular flag.

- To enable all the flags in that group, give the group name followed by **all**.
- To enable all the flags, give 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} |`  
`if-rx {all | if-rx-packet} |`  
`lsa {all | lsa-maxage | lsa-originate} |`  
`overflow {all | lsdB-overflow | lsdB-approaching-overflow} |`  
`retransmit {all | packets | virt-packets} |`  
`rtb {all, rtb-entry-info} |`  
`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 the **group name** followed by that particular flag.
- To disable all the flags in that group, give the group name followed by **all**.
- To disable all the flags, give the command as **trapflags all**.

**Format** `no trapflags {`  
`all |`  
`errors {all | authentication-failure | bad-packet | config-error | virt-`  
`authentication-failure | virt-bad-packet | virt-config-error} |`  
`if-rx {all | if-rx-packet} |`  
`lsa {all | lsa-maxage | lsa-originate} |`  
`overflow {all | lsdB-overflow | lsdB-approaching-overflow} |`  
`retransmit {all | packets | virt-packets} |`  
`rtb {all, rtb-entry-info} |`  
`state-change {all | if-state-change | neighbor-state-change | virtif-state-`  
`change | virtneighbor-state-change}`  
`}`

**Mode** Router OSPF Config

**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
<b>Router ID</b>	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
<b>OSPF Admin Mode</b>	Shows whether the administrative mode of OSPF in the router is enabled or disabled. This is a configured value.
<b>ASBR Mode</b>	Indicates whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes 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).
<b>RFC 1583 Compatibility</b>	Indicates whether 1583 compatibility is enabled or disabled. This is a configured value.
<b>External LSDB Limit</b>	The maximum number of non-default AS-external-LSA (link state advertisement) entries that can be stored in the link-state database.
<b>Exit Overflow Interval</b>	The number of seconds that, after entering overflow state, a router will attempt to leave overflow state.
<b>Spf Delay Time</b>	The number of seconds between two subsequent changes of LSAs, during which time the routing table calculation is delayed.
<b>Spf Hold Time</b>	The number of seconds between two consecutive spf calculations.
<b>Opaque Capability</b>	Shows whether the router is capable of sending Opaque LSAs. This is a configured value.
<b>Autocost Ref BW</b>	Shows the value of auto-cost reference bandwidth configured on the router.
<b>ABR Status</b>	Shows whether the router is an OSPF Area Border Router.
<b>ASBR Status</b>	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).
<b>Stub Router</b>	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 re-originates its own router LSAs, setting the cost of all non-stub interfaces to infinity. To restore OSPF to normal operation, disable and re-enable OSPF.
<b>Exit Overflow Interval</b>	The number of seconds that, after entering overflow state, a router will attempt to leave overflow state.
<b>External LSDB Overflow</b>	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.
<b>External LSA Count</b>	The number of external (LS type 5) link-state advertisements in the link-state database.

Term	Definition
<b>External LSA Checksum</b>	The sum of the LS checksums of external link-state advertisements contained in the link-state database.
<b>AS_OPAQUE LSA Count</b>	Shows the number of AS Opaque LSAs in the link-state database.
<b>AS_OPAQUE LSA Checksum</b>	Shows the sum of the LS Checksums of AS Opaque LSAs contained in the link-state database.
<b>New LSAs Originated</b>	The number of new link-state advertisements that have been originated.
<b>LSAs Received</b>	The number of link-state advertisements received determined to be new instantiations.
<b>LSA Count</b>	The total number of link state advertisements currently in the link state database.
<b>Maximum Number of LSAs</b>	The maximum number of LSAs that OSPF can store.
<b>LSA High Water Mark</b>	The maximum size of the link state database since the system started.
<b>Retransmit List Entries</b>	The total number of LSAs waiting to be acknowledged by all neighbors. An LSA may be pending acknowledgment from more than one neighbor.
<b>Maximum Number of Retransmit Entries</b>	The maximum number of LSAs that can be waiting for acknowledgment at any given time.
<b>Retransmit Entries High Water Mark</b>	The highest number of LSAs that have been waiting for acknowledgment.
<b>External LSDB Limit</b>	The maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database.
<b>Default Metric</b>	Default value for redistributed routes.
<b>Default Passive Setting</b>	Shows whether the interfaces are passive by default.
<b>Default Route Advertise</b>	Indicates whether the default routes received from other source protocols are advertised or not.
<b>Always</b>	Shows whether default routes are always advertised.
<b>Metric</b>	The metric of the routes being redistributed. If the metric is not configured, this field is blank.
<b>Metric Type</b>	Shows whether the routes are External Type 1 or External Type 2.
<b>AutoCost Ref BW</b>	Shows the value of auto-cost reference bandwidth configured on the router.
<b>Maximum Paths</b>	The maximum number of paths that OSPF can report for a given destination.
<b>Redistributing</b>	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.
<b>Source</b>	The source protocol/routes that are being redistributed. Possible values are static, connected, BGP, or RIP.
<b>Tag</b>	The decimal value attached to each external route.
<b>Subnets</b>	For redistributing routes into OSPF, the scope of redistribution for the specified protocol.
<b>Distribute-List</b>	The access list used to filter redistributed routes.

### 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
<b>Router ID</b>	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
<b>OSPF Admin Mode</b>	Shows whether the administrative mode of OSPF in the router is enabled or disabled. This is a configured value.
<b>ASBR Mode</b>	Indicates whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes 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).
<b>RFC 1583 Compatibility</b>	Indicates whether 1583 compatibility is enabled or disabled. This is a configured value.
<b>External LSDB Limit</b>	The maximum number of non-default AS-external-LSA (link state advertisement) entries that can be stored in the link-state database.
<b>Exit Overflow Interval</b>	The number of seconds that, after entering overflow state, a router will attempt to leave overflow state.
<b>Spf Delay Time</b>	The number of seconds between two subsequent changes of LSAs, during which time the routing table calculation is delayed.
<b>Spf Hold Time</b>	The number of seconds between two consecutive spf calculations.
<b>Opaque Capability</b>	Shows whether the router is capable of sending Opaque LSAs. This is a configured value.
<b>Autocost Ref BW</b>	Shows the value of auto-cost reference bandwidth configured on the router.
<b>ABR Status</b>	Shows whether the router is an OSPF Area Border Router.
<b>ASBR Status</b>	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).
<b>Stub Router</b>	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 re-originates its own router LSAs, setting the cost of all non-stub interfaces to infinity. To restore OSPF to normal operation, disable and re-enable OSPF.
<b>Exit Overflow Interval</b>	The number of seconds that, after entering overflow state, a router will attempt to leave overflow state.
<b>External LSDB Overflow</b>	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.
<b>External LSA Count</b>	The number of external (LS type 5) link-state advertisements in the link-state database.
<b>External LSA Checksum</b>	The sum of the LS checksums of external link-state advertisements contained in the link-state database.
<b>AS_OPAQUE LSA Count</b>	Shows the number of AS Opaque LSAs in the link-state database.

Term	Definition
<b>AS_OPAQUE LSA Checksum</b>	Shows the sum of the LS Checksums of AS Opaque LSAs contained in the link-state database.
<b>New LSAs Originated</b>	The number of new link-state advertisements that have been originated.
<b>LSAs Received</b>	The number of link-state advertisements received determined to be new instantiations.
<b>LSA Count</b>	The total number of link state advertisements currently in the link state database.
<b>Maximum Number of LSAs</b>	The maximum number of LSAs that OSPF can store.
<b>LSA High Water Mark</b>	The maximum size of the link state database since the system started.
<b>Retransmit List Entries</b>	The total number of LSAs waiting to be acknowledged by all neighbors. An LSA may be pending acknowledgment from more than one neighbor.
<b>Maximum Number of Retransmit Entries</b>	The maximum number of LSAs that can be waiting for acknowledgment at any given time.
<b>Retransmit Entries High Water Mark</b>	The highest number of LSAs that have been waiting for acknowledgment.
<b>External LSDB Limit</b>	The maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database.
<b>Default Metric</b>	Default value for redistributed routes.
<b>Default Passive Setting</b>	Shows whether the interfaces are passive by default.
<b>Default Route Advertise</b>	Indicates whether the default routes received from other source protocols are advertised or not.
<b>Always</b>	Shows whether default routes are always advertised.
<b>Metric</b>	The metric of the routes being redistributed. If the metric is not configured, this field is blank.
<b>Metric Type</b>	Shows whether the routes are External Type 1 or External Type 2.
<b>AutoCost Ref BW</b>	Shows the value of auto-cost reference bandwidth configured on the router.
<b>Maximum Paths</b>	The maximum number of paths that OSPF can report for a given destination.
<b>Redistributing</b>	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.
<b>Source</b>	The source protocol/routes that are being redistributed. Possible values are static, connected, BGP, or RIP.
<b>Tag</b>	The decimal value attached to each external route.
<b>Subnets</b>	For redistributing routes into OSPF, the scope of redistribution for the specified protocol.
<b>Distribute-List</b>	The access list used to filter redistributed routes.

**Example:** The following shows example CLI display output for the command.

```
(alpha2) #show ip ospf

Router ID.....2.2.2.2
OSPF Admin Mode.....Disable
RFC 1583 Compatibility.....Enable
External LSDB Limit.....No Limit
Exit Overflow Interval.....0
```

```

Spf Delay Time.....5
Spf Hold Time.....10
Opaque Capability.....Disable
AutoCost Ref BW.....100 Mbps
Default Passive Setting.....Disabled
Maximum Paths.....4
Default Metric.....Not configured

Default Route Advertise.....Disabled
Always.....FALSE
Metric.....Not configured
Metric Type.....External Type 2

ABR Status.....Disable
ASBR Status.....Disable
Stub Router.....FALSE
External LSDB Overflow.....FALSE
External LSA Count.....0
External LSA Checksum.....0
AS_OPAQUE LSA Count.....0
AS_OPAQUE LSA Checksum.....0
LSAs Originated.....0
LSAs Received.....0
LSA Count.....0
Maximum Number of LSAs.....18200
LSA High Water Mark.....0
Retransmit List Entries..... 9078
Maximum Number of Retransmit Entries..... 72800
Retransmit Entries High Water Mark..... 72849

```

```
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
<b>Type</b>	The type of the route to the destination. It can be either: <ul style="list-style-type: none"> <li>• intra — Intra-area route</li> <li>• inter — Inter-area route</li> </ul>
<b>Router ID</b>	Router ID of the destination.
<b>Cost</b>	Cost of using this route.
<b>Area ID</b>	The area ID of the area from which this route is learned.
<b>Next Hop</b>	Next hop toward the destination.
<b>Next Hop Intf</b>	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 *<areaid>* identifies the OSPF area that is being displayed.

**Format**            `show ip ospf area <areaid>`

- Modes**
- Privileged EXEC
  - User EXEC

Term	Definition
<b>AreaID</b>	The area id of the requested OSPF area.
<b>External Routing</b>	A number representing the external routing capabilities for this area.
<b>Spf Runs</b>	The number of times that the intra-area route table has been calculated using this area's link-state database.
<b>Area Border Router Count</b>	The total number of area border routers reachable within this area.
<b>Area LSA Count</b>	Total number of link-state advertisements in this area's link-state database, excluding AS External LSA's.
<b>Area LSA Checksum</b>	A number representing the Area LSA Checksum for the specified AreaID excluding the external (LS type 5) link-state advertisements.
<b>Import Summary LSAs</b>	Shows whether to import summary LSAs.
<b>OSPF Stub Metric Value</b>	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
<b>Import Summary LSAs</b>	Shows whether to import summary LSAs into the NSSA.
<b>Redistribute into NSSA</b>	Shows whether to redistribute information into the NSSA.
<b>Default Information Originate</b>	Shows whether to advertise a default route into the NSSA.
<b>Default Metric</b>	The metric value for the default route advertised into the NSSA.
<b>Default Metric Type</b>	The metric type for the default route advertised into the NSSA.
<b>Translator Role</b>	The NSSA translator role of the ABR, which is always or candidate.
<b>Translator Stability Interval</b>	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.
<b>Translator State</b>	Shows whether the ABR translator state is disabled, always, or elected.

**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
<b>Type</b>	The type of the route to the destination. It can be one of the following values: intra — Intra-area route inter — Inter-area route
<b>Router ID</b>	Router ID of the destination.
<b>Cost</b>	Cost of using this route.
<b>Area ID</b>	The area ID of the area from which this route is learned.
<b>Next Hop</b>	Next hop toward the destination.
<b>Next Hop Intf</b>	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 `<areaid>` parameter to display database information about a specific area. Use the optional parameters to specify the type of link state advertisements to display.

Parameter	Description
<b>asbr-summary</b>	Use <code>asbr-summary</code> to show the autonomous system boundary router (ASBR) summary LSAs.
<b>external</b>	Use <code>external</code> to display the external LSAs.
<b>network</b>	Use <code>network</code> to display the network LSAs.
<b>nssa-external</b>	Use <code>nssa-external</code> to display NSSA external LSAs.
<b>opaque-area</b>	Use <code>opaque-area</code> to display area opaque LSAs.
<b>opaque-as</b>	Use <code>opaque-as</code> to display AS opaque LSAs.
<b>opaque-link</b>	Use <code>opaque-link</code> to display link opaque LSAs.
<b>router</b>	Use <code>router</code> to display router LSAs.
<b>summary</b>	Use <code>summary</code> to show the LSA database summary information.
<b>lsid</b>	Use <code>&lt;lsid&gt;</code> to specify the link state ID (LSID). The value of <code>&lt;lsid&gt;</code> can be an IP address or an integer in the range of 0-4294967295.
<b>adv-router</b>	Use <code>adv-router</code> to show the LSAs that are restricted by the advertising router.
<b>self-originate</b>	Use <code>self-originate</code> to display the LSAs in that are self originated. The information below is only displayed if OSPF is enabled

## FL SWITCH GHS CLI

The information below is only displayed if OSPF is enabled.

- Format** `show ip ospf [<areaid>] 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

For each link-type and area, the following information is displayed:

Term	Definition
<b>Link Id</b>	A number that uniquely identifies an LSA that a router originates from all other self originated LSAs of the same LS type.
<b>Adv Router</b>	The Advertising Router. Is a 32 bit dotted decimal number representing the LSDB interface.
<b>Age</b>	A number representing the age of the link state advertisement in seconds.
<b>Sequence</b>	A number that represents which LSA is more recent.
<b>Checksum</b>	The total number LSA checksum.
<b>Options</b>	This is an integer. It indicates that the LSA receives special handling during routing calculations.
<b>Rtr Opt</b>	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
<b>Router</b>	Total number of router LSAs in the OSPF link state database.
<b>Network</b>	Total number of network LSAs in the OSPF link state database.
<b>Summary Net</b>	Total number of summary network LSAs in the database.
<b>Summary ASBR</b>	Number of summary ASBR LSAs in the database.
<b>Type-7 Ext</b>	Total number of Type-7 external LSAs in the database.
<b>Self-Originated Type-7</b>	Total number of self originated AS external LSAs in the OSPFv3 link state database.
<b>Opaque Link</b>	Number of opaque link LSAs in the database.
<b>Opaque Area</b>	Number of opaque area LSAs in the database.
<b>Subtotal</b>	Number of entries for the identified area.
<b>Opaque AS</b>	Number of opaque AS LSAs in the database.
<b>Total</b>	Number of entries for all areas.

**show ip ospf interface**

This command displays the information for the IFO object or virtual interface tables.

- Format**      `show ip ospf interface {<slot/port> | loopback <loopback-id>}`
- Mode**
- Privileged EXEC
  - User EXEC

Term	Definition
<b>IP Address</b>	The IP address for the specified interface.
<b>Subnet Mask</b>	A mask of the network and host portion of the IP address for the OSPF interface.
<b>Secondary IP Address(es)</b>	The secondary IP addresses if any are configured on the interface.
<b>OSPF Admin Mode</b>	States whether OSPF is enabled or disabled on a router interface.
<b>OSPF Area ID</b>	The OSPF Area ID for the specified interface.
<b>OSPF Network Type</b>	The type of network on this interface that the OSPF is running on.
<b>Router Priority</b>	A number representing the OSPF Priority for the specified interface.
<b>Retransmit Interval</b>	A number representing the OSPF Retransmit Interval for the specified interface.
<b>Hello Interval</b>	A number representing the OSPF Hello Interval for the specified interface.
<b>Dead Interval</b>	A number representing the OSPF Dead Interval for the specified interface.
<b>LSA Ack Interval</b>	A number representing the OSPF LSA Acknowledgment Interval for the specified interface.
<b>Transit Delay Interval</b>	A number representing the OSPF Transit Delay for the specified interface.
<b>Authentication Type</b>	The OSPF Authentication Type for the specified interface are: none, simple, and encrypt.
<b>Metric Cost</b>	The cost of the OSPF interface.
<b>Passive Status</b>	Shows whether the interface is passive or not.
<b>OSPF MTU-ignore</b>	Indicates whether to ignore MTU mismatches in database descriptor packets sent from neighboring routers.

The information below will only be displayed if OSPF is enabled.

Term	Definition
<b>OSPF Interface Type</b>	Broadcast LANs, such as Ethernet and IEEE 802.5, take the value <i>broadcast</i> . The OSPF Interface Type will be 'broadcast'.
<b>State</b>	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.
<b>Designated Router</b>	The router ID representing the designated router.
<b>Backup Designated Router</b>	The router ID representing the backup designated router.
<b>Number of Link Events</b>	The number of link events.
<b>Local Link LSAs</b>	The number of Link Local Opaque LSAs in the link-state database.

Term	Definition
<b>Local Link LSA Checksum</b>	The sum of LS Checksums of Link Local Opaque LSAs in the link-state database.

### show ip ospf interface brief

This command displays brief information for the IFO object or virtual interface tables.

**Format**            `show ip ospf interface brief`

- Mode**
- Privileged EXEC
  - User EXEC

Term	Definition
<b>Interface</b>	Valid slot and port number separated by a forward slash.
<b>OSPF Admin Mode</b>	States whether OSPF is enabled or disabled on a router interface.
<b>OSPF Area ID</b>	The OSPF Area Id for the specified interface.
<b>Router Priority</b>	A number representing the OSPF Priority for the specified interface.
<b>Hello Interval</b>	A number representing the OSPF Hello Interval for the specified interface.
<b>Dead Interval</b>	A number representing the OSPF Dead Interval for the specified interface.
<b>Retransmit Interval</b>	A number representing the OSPF Retransmit Interval for the specified interface.
<b>Retransmit Delay Interval</b>	A number representing the OSPF Transit Delay for the specified interface.
<b>LSA Ack Interval</b>	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 information below will only be displayed if OSPF is enabled.

**Format**            `show ip ospf interface stats <slot/port>`

- Modes**
- Privileged EXEC
  - User EXEC

Term	Definition
<b>OSPF Area ID</b>	The area id of this OSPF interface.
<b>Area Border Router Count</b>	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.
<b>AS Border Router Count</b>	The total number of Autonomous System border routers reachable within this area.
<b>Area LSA Count</b>	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
<b>IP Address</b>	The IP address associated with this OSPF interface.
<b>OSPF Interface Events</b>	The number of times the specified OSPF interface has changed its state, or an error has occurred.

Term	Definition
<b>Virtual Events</b>	The number of state changes or errors that occurred on this virtual link.
<b>Neighbor Events</b>	The number of times this neighbor relationship has changed state, or an error has occurred.
<b>External LSA Count</b>	The number of external (LS type 5) link-state advertisements in the link-state database.
<b>Sent Packets</b>	The number of OSPF packets transmitted on the interface.
<b>Received Packets</b>	The number of valid OSPF packets received on the interface.
<b>Discards</b>	The number of received OSPF packets discarded because of an error in the packet or an error in processing the packet.
<b>Bad Version</b>	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.
<b>Source Not On Local Subnet</b>	The number of received packets discarded because the source IP address is not within a subnet configured on a local interface. <b>Note:</b> This field only applies to OSPFv2.
<b>Virtual Link Not Found</b>	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.
<b>Area Mismatch</b>	The number of OSPF packets discarded because the area ID in the OSPF header is not the area ID configured on the ingress interface.
<b>Invalid Destination Address</b>	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.
<b>Wrong Authentication Type</b>	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. <b>Note:</b> This field only applies to OSPFv2.
<b>Authentication Failure</b>	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. <b>Note:</b> This field only applies to OSPFv2.
<b>No Neighbor at Source Address</b>	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. <b>Note:</b> Does not apply to Hellos.
<b>Invalid OSPF Packet Type</b>	The number of OSPF packets discarded because the packet type field in the OSPF header is not a known type.
<b>Hellos Ignored</b>	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.

Table 10 lists the number of OSPF packets of each type sent and received on the interface.

**Table 10: 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 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 *<ip-address>* is the IP address of the neighbor, and when you specify this, detailed information about the neighbor displays. The information below only displays if OSPF is enabled and the interface has a neighbor.

**Format**      `show ip ospf neighbor [interface <slot/port>] [<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
<b>Router ID</b>	The 4-digit dotted-decimal number of the neighbor router.
<b>Priority</b>	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.
<b>IP Address</b>	The IP address of the neighbor.
<b>Interface</b>	The interface of the local router in slot/port format.
<b>State</b>	The state of the neighboring routers. Possible values are: <ul style="list-style-type: none"> <li>• Down - initial state of the neighbor conversation - no recent information has been received from the neighbor.</li> <li>• Attempt - no recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor.</li> <li>• Init - an Hello packet has recently been seen from the neighbor, but bidirectional communication has not yet been established.</li> <li>• 2 way - communication between the two routers is bidirectional.</li> <li>• 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.</li> <li>• Exchange - the router is describing its entire link state database by sending Database Description packets to the neighbor.</li> <li>• 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.</li> <li>• Full - the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.</li> </ul>
<b>Dead Time</b>	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
<b>Interface</b>	Valid slot and port number separated by a forward slash.
<b>Neighbor IP Address</b>	The IP address of the neighbor router.
<b>Interface Index</b>	The interface ID of the neighbor router.

Term	Definition
<b>Area ID</b>	The area ID of the OSPF area associated with the interface.
<b>Options</b>	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 (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.
<b>Router Priority</b>	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.
<b>Dead Timer Due</b>	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.
<b>Up Time</b>	Neighbor uptime; how long since the adjacency last reached the Full state.
<b>State</b>	The state of the neighboring routers.
<b>Events</b>	The number of times this neighbor relationship has changed state, or an error has occurred.
<b>Retransmission Queue Length</b>	An integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.

**Example:** The following shows example CLI display output for the command.

```
(alpha) #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
Retransmission Queue Length.....0
```

### show ip ospf range

This command displays information about the area ranges for the specified *<areaid>*. The *<areaid>* identifies the OSPF area whose ranges are being displayed.

**Format**            `show ip ospf range <areaid>`

- Modes**
- Privileged EXEC
  - User EXEC

Term	Definition
<b>Area ID</b>	The area id of the requested OSPF area.
<b>IP Address</b>	An IP address which represents this area range.
<b>Subnet Mask</b>	A valid subnet mask for this area range.
<b>Lsdb Type</b>	The type of link advertisement associated with this area range.
<b>Advertisement</b>	The status of the advertisement. Advertisement has two possible settings: enabled or disabled.

### 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 table lists how long ago the SPF ran, how long the SPF took, and the reasons why the SPF was scheduled.

**Format**            `show ip ospf statistics`

- Modes**
- Privileged EXEC
  - User EXEC

Term	Definition
<b>Delta T</b>	How long ago the SPF ran. The time is in the format hh:mm:ss, giving the hours, minutes, and seconds since the SPF run.
<b>SPF Duration</b>	How long the SPF took in milliseconds.
<b>Reason</b>	The reason the SPF was scheduled. Reason codes are as follows: <ul style="list-style-type: none"> <li>• R - a router LSA has changed</li> <li>• N - a network LSA has changed</li> <li>• SN - a type 3 network summary LSA has changed</li> <li>• SA - a type 4 ASBR summary LSA has changed</li> <li>• X - a type 5 or type 7 external LSA has changed</li> </ul>

### 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
<b>Area ID</b>	A 32-bit identifier for the created stub area.
<b>Type of Service</b>	The type of service associated with the stub metric. FL SWITCH GHS Firmware only supports Normal TOS.
<b>Metric Val</b>	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.
<b>Import Summary LSA</b>	Controls the import of summary LSAs into stub areas.

**show ip ospf virtual-link**

This command displays the OSPF Virtual Interface information for a specific area and neighbor. The *<areaid>* parameter identifies the area and the *<neighbor>* parameter identifies the neighbor's Router ID.

**Format**            `show ip ospf virtual-link <areaid> <neighbor>`

- Modes**
- Privileged EXEC
  - User EXEC

Term	Definition
<b>Area ID</b>	The area id of the requested OSPF area.
<b>Neighbor Router ID</b>	The input neighbor Router ID.
<b>Hello Interval</b>	The configured hello interval for the OSPF virtual interface.
<b>Dead Interval</b>	The configured dead interval for the OSPF virtual interface.
<b>Iftransit Delay Interval</b>	The configured transit delay for the OSPF virtual interface.
<b>Retransmit Interval</b>	The configured retransmit interval for the OSPF virtual interface.
<b>Authentication Type</b>	The configured authentication type of the OSPF virtual interface.
<b>State</b>	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.
<b>Neighbor State</b>	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
<b>Area ID</b>	The area id of the requested OSPF area.
<b>Neighbor</b>	The neighbor interface of the OSPF virtual interface.
<b>Hello Interval</b>	The configured hello interval for the OSPF virtual interface.
<b>Dead Interval</b>	The configured dead interval for the OSPF virtual interface.
<b>Retransmit Interval</b>	The configured retransmit interval for the OSPF virtual interface.
<b>Transit Delay</b>	The configured transit delay for the OSPF virtual interface.

## DISPLAY

The following CLI commands will be implemented for display contrast adjustment:

In Privileged EXEC mode:

`display-contrast <contrast value>`

The user may enter a contrast value which will be applied to the display immediately and will be stored in NV-Ram immediately as well.

Valid values are 1 to 255

`show display contrast`

The user can show the actual valid display contrast value.

## PORT CONFIGURATION COMMANDS

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

### interface

This command gives you access to the Interface Config mode, which allows you to enable or modify the operation of an interface (port).

**Format**            `interface <slot/port>`  
**Mode**              Global Config

**Format**            `interface <slot/port>`  
**Mode**              Global Config

## BASIC PORT FEATURES

The optional CLI does provide the following informational commands:

`show port all` - does print a table with the basic parameters: port identifier, Mirroring parameter, Administrative Mode, configured mode, speed/duplex information, Link status

`show port <slot/port>` - does print only one table row of the given port

`show port description <slot/port>` - does print Port number, Port Name and MAC address of the given port

`show port full all` - does print detailed information of all ports: port identifier, Mirroring parameter, Administrative Mode, configured mode, speed/duplex information, Link status, Port Name, Media Type, Module

show port full <slot/port> - does print detailed information of the given port

The following commands are used in interface configuration mode:

(no) shutdown - to disable (enable) the port

(no) auto-negotiate - to enable (disable) autonegotiation

speed <speed> <duplex> - set speed to 10 or 100 and duplex to full-duplex or half-duplex (if autonegotiation is still enabled, a warning message will appear)

description <text> - set the Port Name

(no) link-monitoring - enable (disable) link monitoring

classofservice dot1p-mapping <priority> - set default Priority value (an error message will appear if the value is out of range)

## AUTO-NEGOTIATE

This command enables automatic negotiation on a port.

<b>Default</b>	enabled
<b>Format</b>	<code>auto-negotiate</code>
<b>Mode</b>	Interface Config

*no auto-negotiate*

This command disables automatic negotiation on a port.



**Note:** Automatic sensing is disabled when automatic negotiation is disabled.

<b>Format</b>	<code>no auto-negotiate</code>
<b>Mode</b>	Interface Config

## auto-negotiate all

This command enables automatic negotiation on all ports.

<b>Default</b>	enabled
<b>Format</b>	<code>auto-negotiate all</code>
<b>Mode</b>	Global Config

*no auto-negotiate all*

This command disables automatic negotiation on all ports.

<b>Format</b>	<code>no auto-negotiate all</code>
<b>Mode</b>	Global Config

### description

Use this command to create an alpha-numeric description of the port.

**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 FL SWITCH GHS Firmware 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 143](#).

**Default**            1518 (untagged)  
**Format**            `mtu <1518-9216>`  
**Mode**             Interface Config

### *no mtu*

This command sets the default MTU size (in bytes) for the interface.

**Format**            `no mtu`  
**Mode**             Interface Config

### shutdown

This command disables a port. speed



**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

This command sets the speed and duplex setting for the interface.

**Format**            `speed {<100 | 10> <half-duplex | full-duplex>}`  
**Mode**             Interface Config

Acceptable Values	Definition
100h	100BASE-T half duplex
100f	100BASE-T full duplex
10h	10BASE-T half duplex
10f	10BASE-T full duplex

**fast start-up**

### 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

Acceptable Values	Definition
100h	100BASE-T half duplex
100f	100BASE-T full duplex
10h	10BASE-T half duplex
10f	10BASE-T full duplex

### show port

This command displays port information.

**Format**            `show port {<slot/port> | all}`  
**Mode**             Privileged EXEC

Term	Definition
<b>Interface</b>	Valid slot and port number separated by a forward slash.
<b>Type</b>	If not blank, this field indicates that this port is a special type of port. The possible values are: <ul style="list-style-type: none"> <li>• <b>Mirror</b> - this port is a monitoring port. For more information, see <a href="#">“Port Mirroring” on page 86</a>.</li> <li>• <b>PC Mbr</b>- this port is a member of a port-channel (LAG).</li> <li>• <b>Probe</b> - this port is a probe port.</li> </ul>
<b>Admin Mode</b>	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.
<b>Physical Mode</b>	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.
<b>Physical Status</b>	The port speed and duplex mode.
<b>Link Status</b>	The Link is up or down.
<b>Link Trap</b>	This object determines whether or not to send a trap when link status changes. The factory default is enabled.
<b>LACP Mode</b>	LACP is enabled or disabled on this port.

## SPANNING TREE PROTOCOL (STP) 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 disabled by default. When you enable STP on the switch, STP is still disabled on each port.



**Note:** If STP is disabled, the system does not forward BPDU messages.

### **spanning-tree**

This command sets the spanning-tree operational mode to enabled.

**Default** disabled  
**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 bpdupfilter**

Use this command to enable BPDU Filter on the interface.

**Default** disabled  
**Format** `spanning-tree bpdupfilter`  
**Mode** Interface Config

### *no spanning-tree bpdupfilter*

Use this command to disable BPDU Filter on the interface.

**Default** disabled  
**Format** `no spanning-tree bpdupfilter`  
**Mode** Interface Config

**spanning-tree bpdupfilter default**

Use this command to enable BPDU Filter on all the edge port interfaces.

**Default** disabled  
**Format** `spanning-tree bpdupfilter`  
**Mode** Global Config

*no spanning-tree bpdupfilter default*

Use this command to disable BPDU Filter on all the edge port interfaces.

**Default** disabled  
**Format** `no spanning-tree bpdupfilter default`  
**Mode** Global Config

**spanning-tree bpduflood**

Use this command to enable BPDU Flood on the interface.

**Default** disabled  
**Format** `spanning-tree bpduflood`  
**Mode** Interface Config

*no spanning-tree bpduflood*

Use this command to disable BPDU Flood on the interface.

**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 `<slot/port>` parameter to transmit a BPDU from a specified interface, or use the `all` keyword to transmit 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 {<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>` 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 <0-65535>`  
**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 edgeport**

This command specifies that this port 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 forceversion**

This command sets the Force Protocol Version parameter to a new value.

**Default** 802.1s

**Format** `spanning-tree forceversion <802.1d | 802.1s | 802.1w>`

**Mode** Global Config

- Use 802.1d to specify that the switch transmits ST BPDUs rather than MST BPDUs (IEEE 802.1d functionality supported).
- Use 802.1s to specify that the switch transmits MST BPDUs (IEEE 802.1s functionality supported).
- Use 802.1w to specify that the switch transmits RST BPDUs rather than MST BPDUs (IEEE 802.1w functionality supported).

*no spanning-tree forceversion*

This command sets the Force Protocol Version parameter to the default value.

**Format** `no spanning-tree forceversion`

**Mode** Global 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 <4-30>`  
**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 hello-time

This command sets the Admin Hello Time parameter to a new value for the common and internal spanning tree. The hello time *<value>* is in whole seconds within a range of 1 to 10, with the value being less than or equal to *(Bridge Max Age / 2) - 1*.

**Default** 2  
**Format** `spanning-tree hello-time <1-10>`  
**Mode** Interface Config

### *no spanning-tree hello-time*

This command sets the admin Hello Time parameter for the common and internal spanning tree to the default value.

**Format** `no spanning-tree hello-time`  
**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  $2 \times (\text{Bridge Forward Delay} - 1)$ .

**Default** 20  
**Format** `spanning-tree max-age <6-40>`  
**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 MSTP Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is a range from 1 to 127.

**Default**        20  
**Format**        `spanning-tree max-hops <1-127>`  
**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 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 **external-cost** option, this command sets the external-path cost for MST instance '0' i.e. CIST instance. You can set the external cost as a number in the range of 1 to 200000000 or **auto**. If you specify **auto**, the external 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.

<b>Default</b>	<ul style="list-style-type: none"> <li>• cost—auto</li> <li>• external-cost—auto</li> <li>• port-priority—128</li> </ul>
<b>Format</b>	<b>spanning-tree mst</b> <mstid> {{cost <1-200000000>   auto}   {external-cost <1-200000000>   auto}   port-priority <0-240>}
<b>Mode</b>	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 **external-cost**, this command sets the external path cost for this port for mst '0' instance, 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.

<b>Format</b>	<b>no spanning-tree mst</b> <mstid> <cost   external-cost   port-priority>
<b>Mode</b>	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.

<b>Default</b>	none
<b>Format</b>	<b>spanning-tree mst instance</b> <mstid>
<b>Mode</b>	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 61440 in increments of 4096.

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 61440. 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> <0-61440>`  
**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 a VLAN so that the VLAN is no longer associated with the common and internal spanning tree. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance. The *<vlanid>* corresponds to an existing VLAN ID.

**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 a VLAN so that the VLAN is again be associated with the common and internal spanning tree. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance. The *<vlanid>* corresponds to an existing VLAN ID.

**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.

**Default**        disabled  
**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.

**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**        disabled  
**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

**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
<b>Bridge Priority</b>	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.
<b>Bridge Identifier</b>	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
<b>Time Since Topology Change</b>	Time in seconds.
<b>Topology Change Count</b>	Number of times changed.
<b>Topology Change</b>	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.
<b>Designated Root</b>	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
<b>Root Path Cost</b>	Value of the Root Path Cost parameter for the common and internal spanning tree.
<b>Root Port Identifier</b>	Identifier of the port to access the Designated Root for the CST
<b>Root Port Max Age</b>	Derived value.
<b>Root Port Bridge Forward Delay</b>	Derived value
<b>Hello Time</b>	Configured value of the parameter for the CST.
<b>Bridge Hold Time</b>	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).
<b>Bridge Max Hops</b>	Bridge max-hops count for the device.
<b>CST Regional Root</b>	Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
<b>Regional Root Path Cost</b>	Path Cost to the CST Regional Root.
<b>Associated FIDs</b>	List of forwarding database identifiers currently associated with this instance.
<b>Associated VLANs</b>	List of VLAN IDs currently associated with this instance.

### 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
<b>Bridge Priority</b>	Configured value.
<b>Bridge Identifier</b>	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
<b>Bridge Max Age</b>	Configured value.

Term	Definition
<b>Bridge Max Hops</b>	Bridge max-hops count for the device.
<b>Bridge Hello Time</b>	Configured value.
<b>Bridge Forward Delay</b>	Configured value.
<b>Bridge Hold Time</b>	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).

### show spanning-tree interface

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The *<slot/port>* is the desired switch port. The following details are displayed on execution of the command.

**Format**            `show spanning-tree interface <slot/port>`

- Mode**
- Privileged EXEC
  - User EXEC

Term	Definition
<b>Hello Time</b>	Admin hello time for this port.
<b>Port Mode</b>	Enabled or disabled.
<b>BPDU Filter</b>	Enabled or disabled.
<b>BPDU Flood</b>	Enabled or disabled.
<b>BPDU Guard</b>	Enabled or disabled.
<b>Root Guard</b>	Enabled or disabled.
<b>Port Up Time Since Counters Last Cleared</b>	Time since port was reset, displayed in days, hours, minutes, and seconds.
<b>STP BPDUs Transmitted</b>	Spanning Tree Protocol Bridge Protocol Data Units sent.
<b>STP BPDUs Received</b>	Spanning Tree Protocol Bridge Protocol Data Units received.
<b>RST BPDUs Transmitted</b>	Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.
<b>RST BPDUs Received</b>	Rapid Spanning Tree Protocol Bridge Protocol Data Units received.
<b>MSTP BPDUs Transmitted</b>	Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.
<b>MSTP BPDUs Received</b>	Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

### 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 *<slot/port>* is the desired switch port.

<b>Format</b>	<code>show spanning-tree mst port detailed &lt;mstid&gt; &lt;slot/port&gt;</code>
<b>Mode</b>	<ul style="list-style-type: none"> <li>• Privileged EXEC</li> <li>• User EXEC</li> </ul>

Term	Definition
<b>MST Instance ID</b>	The ID of the existing MST instance.
<b>Port Identifier</b>	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.
<b>Port Priority</b>	The priority for a particular port within the selected MST instance. The port priority is displayed in multiples of 16.
<b>Port Forwarding State</b>	Current spanning tree state of this port.
<b>Port Role</b>	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
<b>Auto-Calculate Port Path Cost</b>	Indicates whether auto calculation for port path cost is enabled.
<b>Port Path Cost</b>	Configured value of the Internal Port Path Cost parameter.
<b>Auto-Calculate External Port Path Cost</b>	Indicates whether auto calculation for external port path cost is enabled.
<b>External Port Path Cost</b>	Configured value of the external Port Path Cost parameter.
<b>Designated Root</b>	The Identifier of the designated root for this port.
<b>Designated Port Cost</b>	Path Cost offered to the LAN by the Designated Port.
<b>Designated Bridge</b>	Bridge Identifier of the bridge with the Designated Port.
<b>Designated Port Identifier</b>	Port on the Designated Bridge that offers the lowest cost to the LAN.

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 *<slot/port>* is the desired switch port. In this case, the following are displayed.

Term	Definition
<b>Port Identifier</b>	The port identifier for this port within the CST.
<b>Port Priority</b>	The priority of the port within the CST.
<b>Port Forwarding State</b>	The forwarding state of the port within the CST.
<b>Port Role</b>	The role of the specified interface within the CST.
<b>Port Path Cost</b>	The configured path cost for the specified interface.
<b>Designated Root</b>	Identifier of the designated root for this port within the CST.
<b>Designated Port Cost</b>	Path Cost offered to the LAN by the Designated Port.
<b>Designated Bridge</b>	The bridge containing the designated port.
<b>Designated Port Identifier</b>	Port on the Designated Bridge that offers the lowest cost to the LAN.

Term	Definition
<b>Topology Change Acknowledgement</b>	Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.
<b>Hello Time</b>	The hello time in use for this port.
<b>Edge Port</b>	The configured value indicating if this port is an edge port.
<b>Edge Port Status</b>	The derived value of the edge port status. True if operating as an edge port; false otherwise.
<b>Point To Point MAC Status</b>	Derived value indicating if this port is part of a point to point link.
<b>CST Regional Root</b>	The regional root identifier in use for this port.
<b>CST Port Cost</b>	The configured path cost for this port.

### 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 *{<slot/port> | all}* indicates the desired switch port or all ports.

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> {<slot/port> | all}`

- Mode**
- Privileged EXEC
  - User EXEC

Term	Definition
<b>MST Instance ID</b>	The MST instance associated with this port.
<b>Interface</b>	Valid slot and port number separated by a forward slash.
<b>Type</b>	Currently not used.
<b>STP State</b>	The forwarding state of the port in the specified spanning tree instance.
<b>Port Role</b>	The role of the specified port within the spanning tree.
<b>Link Status</b>	The operational status of the link. Possible values are “Up” or “Down”.
<b>Link Trap</b>	The link trap configuration for the specified interface.

### 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
<b>MST Instance ID List</b>	List of multiple spanning trees IDs currently configured.
<b>For each MSTID:</b>	<ul style="list-style-type: none"> <li>List of forwarding database identifiers associated with this instance.</li> <li>List of VLAN IDs associated with this instance.</li> </ul>
	<ul style="list-style-type: none"> <li>Associated FIDs</li> <li>Associated VLANs</li> </ul>

### 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
<b>Spanning Tree Adminmode</b>	Enabled or disabled.
<b>Spanning Tree Version</b>	Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter.
<b>BPDU Guard Mode</b>	Enabled or disabled.
<b>BPDU Filter Mode</b>	Enabled or disabled.
<b>Configuration Name</b>	Identifier used to identify the configuration currently being used.
<b>Configuration Revision Level</b>	Identifier used to identify the configuration currently being used.
<b>Configuration Digest Key</b>	Identifier used to identify the configuration currently being used.
<b>MST Instances</b>	List of all multiple spanning tree instances configured on the switch.

### show spanning-tree vlan

This command displays the association between a VLAN and a multiple spanning tree instance. The `<vlanid>` corresponds to an existing VLAN ID.

**Format** `show spanning-tree vlan <vlanid>`

**Mode**

- Privileged EXEC
- User EXEC

Term	Definition
<b>VLAN Identifier</b>	The VLANs associated with the selected MST instance.
<b>Associated Instance</b>	Identifier for the associated multiple spanning tree instance or "CST" if associated with the common and internal spanning tree.

The following commands are added for Large-Tree-Support and Fast-Ring-Detection.

Mode	Command
<b>Global Config</b>	
	fast-ring-detection
	large-tree-support
<b>Show Commands</b>	
	show spanning-tree fast-rings

## 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.

**Default**      1  
**Format**      `network mgmt_vlan <1-4069>`  
**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). VLAN range is 2-4094.

**Format**      `vlan <2-4094>`  
**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 range is 2-4094.

**Format** `no vlan <2-4094>`

**Mode** VLAN Config

**vlan acceptframe**

This command sets the frame acceptance mode per interface. 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. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

**Default** all

**Format** `vlan acceptframe {vlanonly | all}`

**Mode** Interface Config

*no vlan acceptframe*

This command resets the frame acceptance mode for the interface to the default value.

**Format** `no vlan acceptframe`

**Mode** Interface Config

**vlan ingressfilter**

This command enables 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.

**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 makestatic**

This command changes a dynamically created VLAN (one that is created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2-4094.

**Format** `vlan makestatic <2-4094>`

**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 ID is a valid VLAN identification number. ID range is 1-4094.

- Default**
- VLAN ID 1 - default
  - other VLANS - blank string

**Format** `vlan name <2-4094> <name>`

**Mode** VLAN Config

*no vlan name*

This command sets the name of a VLAN to a blank string.

**Format** `no vlan name <2-4094>`

**Mode** VLAN Config

**vlan participation**

This command configures the degree of participation for a specific interface in a VLAN. The ID is a valid VLAN identification number, and the interface is a valid interface number .

**Format** `vlan participation {exclude | include | auto} <1-4094>`

**Mode** Interface Config

Participation options are:

Participation Options	Definition
<b>include</b>	The interface is always a member of this VLAN. This is equivalent to registration fixed.
<b>exclude</b>	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
<b>auto</b>	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 participation all**

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number.

**Format** `vlan participation all {exclude | include | auto} <1-4094>`  
**Mode** Global Config

You can use the following participation options:

Participation Options	Definition
<b>include</b>	The interface is always a member of this VLAN. This is equivalent to registration fixed.
<b>exclude</b>	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
<b>auto</b>	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.

**Default** all  
**Format** `vlan port acceptframe all {vlanonly | all}`  
**Mode** Global Config

The modes defined as follows:

Mode	Definition
<b>VLAN Only mode</b>	Untagged frames or priority frames received on this interface are discarded.
<b>Admit All mode</b>	Untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port.

With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

*no vlan port acceptframe all*

This command sets the frame acceptance mode for all interfaces to Admit All. 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. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

**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 interface.

**Default** 1  
**Format** `vlan port pvid all <1-4094>`  
**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 ID is a valid VLAN identification number.

**Format** `vlan port tagging all <1-4094>`  
**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 ID is a valid VLAN identification number.

**Format**            `no vlan port tagging all`

**Mode**             Global Config

**vlan pvid**

This command changes the VLAN ID per interface.

**Default**           1

**Format**           `vlan pvid <1-4094>`

**Mode**             Interface Config

*no vlan pvid*

This command sets the VLAN ID per interface to 1.

**Format**           `no vlan pvid`

**Mode**             Interface Config

**vlan tagging**

This command configures the tagging behavior for a specific interface 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 ID is a valid VLAN identification number.

**Format**           `vlan tagging <1-4094>`

**Mode**             Interface Config

*no vlan tagging*

This command configures the tagging behavior for a specific interface in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

**Format**           `no vlan tagging <1-4094>`

**Mode**             Interface Config

**vlan tagging mode**

**Default**           transparent

**Format**        `mode tagging`  
**Mode**            VLAN database

**Default**        transparent  
**Format**        `mode transparent`  
**Mode**            VLAN database

**show vlan mode**

**Format**        `show vlan mode`  
**Mode**            Privileged EXEC

**show vlan**

This command displays detailed information, including interface information, for a specific VLAN. The ID is a valid VLAN identification number.

**Format**        `show vlan <vlanid>`  
**Mode**            • Privileged EXEC  
                   • User EXEC

Term	Definition
<b>VLAN ID</b>	There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4094.
<b>VLAN Name</b>	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.
<b>VLAN Type</b>	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration).
<b>Interface</b>	Valid slot and port number separated by a forward slash. It is possible to set the parameters for all ports by using the selectors on the top line.
<b>Current</b>	The degree of participation of this port in this VLAN. The permissible values are: <ul style="list-style-type: none"> <li>• <b>Include</b> - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.</li> <li>• <b>Exclude</b> - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.</li> <li>• <b>Autodetect</b> - 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.</li> </ul>
<b>Configured</b>	The configured degree of participation of this port in this VLAN. The permissible values are: <ul style="list-style-type: none"> <li>• <b>Include</b> - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.</li> <li>• <b>Exclude</b> - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.</li> <li>• <b>Autodetect</b> - 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.</li> </ul>

Term	Definition
<b>Tagging</b>	The tagging behavior for this port in this VLAN. <ul style="list-style-type: none"> <li>• <b>Tagged</b> - Transmit traffic for this VLAN as tagged frames.</li> <li>• <b>Untagged</b> - Transmit traffic for this VLAN as untagged frames.</li> </ul>

### show vlan brief

This command displays a list of all configured VLANs.

<b>Format</b>	<code>show vlan brief</code>
<b>Mode</b>	<ul style="list-style-type: none"> <li>• Privileged EXEC</li> <li>• User EXEC</li> </ul>

Term	Definition
<b>VLAN ID</b>	There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1 to 4094.
<b>VLAN Name</b>	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.
<b>VLAN Type</b>	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or a Dynamic (one that is created by GVRP registration).

### show vlan port

This command displays VLAN port information.

<b>Format</b>	<code>show vlan port {&lt;slot/port&gt;   all}</code>
<b>Mode</b>	<ul style="list-style-type: none"> <li>• Privileged EXEC</li> <li>• User EXEC</li> </ul>

Term	Definition
<b>Interface</b>	Valid slot and port number separated by a forward slash. It is possible to set the parameters for all ports by using the selectors on the top line.
<b>Port VLAN ID</b>	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.
<b>Acceptable Frame Types</b>	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.
<b>Ingress Filtering</b>	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.
<b>GVRP</b>	May be enabled or disabled.
<b>Default Priority</b>	The 802.1p priority assigned to tagged packets arriving on the port.

## PROVISIONING (IEEE 802.1P) COMMANDS

This section describes the commands you use to configure provisioning, 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

## 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).

### show garp

This command displays GARP information.

**Format** `show garp`  
**Mode**

- Privileged EXEC
- User EXEC

Term	Definition
<b>GMRP Admin Mode</b>	The administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.
<b>GVRP Admin Mode</b>	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) or all ports (Global Config mode).

**Default** disabled  
**Format** `set gvrp interfacemode`  
**Mode**

- Interface Config
- Global Config

*no set gvrp interfacemode*

This command disables GVRP on a single port (Interface Config mode) or all ports (Global Config mode). If GVRP is disabled, Join Time, Leave Time and Leave All Time have no effect.

**Format** `no set gvrp interfacemode`  
**Mode**

- Interface Config
- Global Config

**show gvrp configuration**

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

**Format** `show gvrp configuration {<slot/port> | all}`  
**Mode**

- Privileged EXEC
- User EXEC

Term	Definition
<b>Interface</b>	Valid slot and port number separated by a forward slash.
<b>Join Timer</b>	The interval between the transmission of GARP PDUs registering (or re-registering) 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).
<b>Leave Timer</b>	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).
<b>LeaveAll Timer</b>	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).
<b>Port GMRP Mode</b>	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) 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 {<slot/port> | all}`

**Mode**

- Privileged EXEC
- User EXEC

Term	Definition
<b>Interface</b>	The slot/port of the interface that this row in the table describes.
<b>Join Timer</b>	The interval between the transmission of GARP PDUs registering (or re-registering) 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).
<b>Leave Timer</b>	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).
<b>LeaveAll Timer</b>	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).
<b>Port GMRP Mode</b>	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.

## PORT-BASED NETWORK ACCESS CONTROL COMMANDS

This section describes the commands you use to configure port-based network access control (802.1x). Port-based network access control allows you to permit access to network services only to and devices that are authorized and authenticated.

### clear dot1x statistics

This command resets the 802.1x statistics for the specified port or for all ports.

**Format** `clear dot1x statistics {<slot/port> | all}`  
**Mode** Privileged EXEC

### clear radius statistics

This command is used to clear all RADIUS statistics.

**Format** `clear radius statistics`  
**Mode** Privileged EXEC

### dot1x guest-vlan

This command configures VLAN as guest vlan on a per port basis. The command specifies an active VLAN as an IEEE 802.1x guest VLAN. The range is 1 to the maximumVLAN 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'. If the control mode is not 'auto' an error will be returned.

**Format** `dot1x initialize <slot/port>`

**Mode** Privileged EXEC

### **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. The *<count>* value 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 port-control**

This command sets the authentication mode to use on the specified port. Select *force-unauthorized* to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select *force-authorized* to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select *auto* 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.

**Default** auto  
**Format** `dot1x port-control {force-unauthorized | force-authorized | auto}`  
**Mode** Interface Config

*no dot1x port-control*

This command sets the authentication mode on the specified port to the default value.

**Format** `no dot1x port-control`  
**Mode** Interface Config

### **dot1x re-authenticate**

This command begins the re-authentication sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

**Format** `dot1x re-authenticate <slot/port>`  
**Mode** Privileged EXEC

### **dot1x re-authentication**

This command enables re-authentication of the supplicant for the specified port.

**Default** disabled  
**Format** `dot1x re-authentication`  
**Mode** Interface Config

*no dot1x re-authentication*

This command disables re-authentication 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 timeout**

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port. Depending on the token used and the value (in seconds) passed, various timeout configurable parameters are set. The following tokens are supported:

Tokens	Definition
<b>reauth-period</b>	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when re-authentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.
<b>quiet-period</b>	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.
<b>tx-period</b>	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.
<b>supp-timeout</b>	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.
<b>server-timeout</b>	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**
- reauth-period: 3600 seconds
  - quiet-period: 60 seconds
  - tx-period: 30 seconds
  - supp-timeout: 30 seconds
  - server-timeout: 30 seconds

**Format** `dot1x timeout {{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 {reauth-period | quiet-period | tx-period | supp-timeout | server-timeout}`

**Mode** Interface Config

**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 {<slot/port> | all} | detail <slot/port> | statistics <slot/port>}]`

**Mode** Privileged EXEC

If you do not use the optional parameters *<unit/slot/port>* or *<vlanid>*, the command displays the global dot1x mode and the Guest VLAN supplicant mode.

Term	Definition
<b>Administrative mode</b>	Indicates whether authentication control on the switch is enabled or disabled.
<b>Supplicant Allowed in Guest VLAN</b>	Indicates whether Guest VLAN is enabled or disabled.

If you use the optional parameter *summary {<slot/port> | all}*, the dot1x configuration for the specified port or all ports are displayed.

Term	Definition
<b>Port</b>	The interface whose configuration is displayed.
<b>Control Mode</b>	The configured control mode for this port. Possible values are force-unauthorized   force-authorized   auto.
<b>Operating Control Mode</b>	The control mode under which this port is operating. Possible values are authorized   unauthorized.
<b>Reauthentication Enabled</b>	Indicates whether re-authentication is enabled on this port.
<b>Key Transmission Enabled</b>	Indicates if the key is transmitted to the supplicant for the specified port.

The command `show dot1x detail <unit/slot/port>` displays guest-vlan. The configured guest-vlan ID is displayed. If the optional parameter `'detail <slot/port>'` is used, the detailed dot1x configuration for the specified port is displayed.

Term	Definition
<b>Port</b>	The interface whose configuration is displayed.
<b>Protocol Version</b>	The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.
<b>PAE Capabilities</b>	The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.

Term	Definition
<b>Authenticator PAE State</b>	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
<b>Backend Authentication State</b>	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.
<b>Quiet Period</b>	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.
<b>Transmit Period</b>	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.
<b>Guest-VLAN ID</b>	The guest VLAN identifier configured on the interface.
<b>Guest-Vlan Operational Mode</b>	Indicates whether guest-vlan operational mode is enabled or disabled.
<b>Supplicant Timeout</b>	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.
<b>Server Timeout</b>	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.
<b>Maximum Requests</b>	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.
<b>Vlan-assigned</b>	The VLAN assigned to the port by the radius server.
<b>Reauthentication Period</b>	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.
<b>Reauthentication Enabled</b>	Indicates if reauthentication is enabled on this port. Possible values are "True" or "False".
<b>Key Transmission Enabled</b>	Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.
<b>Control Direction</b>	The control direction for the specified port or ports. Possible values are both or in.

If you use the optional parameter `statistics <slot/port>`, the following dot1x statistics for the specified port appear.

Term	Definition
<b>Port</b>	The interface whose statistics are displayed.
<b>EAPOL Frames Received</b>	The number of valid EAPOL frames of any type that have been received by this authenticator.
<b>EAPOL Frames Transmitted</b>	The number of EAPOL frames of any type that have been transmitted by this authenticator.
<b>EAPOL Start Frames Received</b>	The number of EAPOL start frames that have been received by this authenticator.
<b>EAPOL Logoff Frames Received</b>	The number of EAPOL logoff frames that have been received by this authenticator.
<b>Last EAPOL Frame Version</b>	The protocol version number carried in the most recently received EAPOL frame.
<b>Last EAPOL Frame Source</b>	The source MAC address carried in the most recently received EAPOL frame.

Term	Definition
<b>EAP Response/Id Frames Received</b>	The number of EAP response/identity frames that have been received by this authenticator.
<b>EAP Response Frames Received</b>	The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.
<b>EAP Request/Id Frames Transmitted</b>	The number of EAP request/identity frames that have been transmitted by this authenticator.
<b>EAP Request Frames Transmitted</b>	The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.
<b>Invalid EAPOL Frames Received</b>	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
<b>EAP Length Error Frames Received</b>	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

## STORM-CONTROL COMMANDS

This section describes commands you use to configure storm control and view storm-control configuration information. 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. The Storm Control feature can help maintain network performance.

### storm-control broadcast

Use this command to enable broadcast storm recovery mode for a specific interface. 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.

<b>Default</b>	disabled
<b>Format</b>	<code>storm-control broadcast</code>
<b>Mode</b>	Interface Config

*no storm-control broadcast*

Use this command to disable broadcast storm recovery mode for a specific interface.

<b>Format</b>	<code>no storm-control broadcast</code>
<b>Mode</b>	Interface Config

### storm-control broadcast all

This command enables broadcast storm recovery mode for all interfaces. 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 all`  
**Mode** Global Config

*no storm-control broadcast all*

This command disables broadcast storm recovery mode for all interfaces.

**Format** `no storm-control broadcast all`  
**Mode** Global Config

### **storm-control multicast**

This command enables multicast storm recovery mode for an interface. 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** Interface Config

*no storm-control multicast*

This command disables multicast storm recovery mode for an interface.

**Format** `no storm-control multicast`  
**Mode** Interface Config

### **storm-control multicast rate**

This command configures the multicast storm recovery threshold in terms of percentage of the interface speed for an interface 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.

**Default** 5  
**Format** `storm-control multicast rate <0-100>`  
**Mode** Interface Config

*no storm-control multicast rate*

This command sets the multicast storm recovery threshold to the default value for an interface and disables multicast storm recovery.

**Format**        `no storm-control multicast`  
**Mode**            Interface Config

**storm-control multicast all**

This command enables multicast storm recovery mode for all interfaces. 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 all`  
**Mode**            Global Config

*no storm-control multicast all*

This command disables multicast storm recovery mode for all interfaces.

**Format**        `no storm-control multicast all`  
**Mode**            Global Config

**storm-control multicast all rate**

This command configures the multicast storm recovery threshold, in terms of percentage of the interface speed, for all interfaces 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.

**Default**        5  
**Format**        `storm-control multicast all rate`  
**Mode**            Global Config

*no storm-control multicast all rate*

This command sets the multicast storm recovery threshold to the default value for all interfaces and disables multicast storm recovery.

**Format**        `no storm-control multicast all rate`  
**Mode**            Global Config

**storm-control unicast**

This command enables unicast storm recovery mode for an interface. 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** Interface Config

*no storm-control unicast*

This command disables unicast storm recovery mode for an interface.

**Format** `no storm-control unicast`  
**Mode** Interface Config

### **storm-control unicast rate**

This command configures the unicast storm recovery threshold in terms of percentage of the interface speed for an interface, 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.

**Default** 5  
**Format** `storm-control unicast rate`  
**Mode** Interface Config

*no storm-control unicast rate*

This command sets the unicast storm recovery threshold to the default value for an interface and disables unicast storm recovery.

**Format** `no storm-control unicast rate`  
**Mode** Interface Config

### **storm-control unicast all**

This command enables unicast storm recovery mode for all interfaces. 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 all`

**Mode** Global Config

*no storm-control unicast all*

This command disables unicast storm recovery mode for all interfaces.

**Format** `no storm-control unicast all`

**Mode** Global Config

### **storm-control unicast all rate**

This command configures the unicast storm recovery threshold in terms of percentage of the interface speed for an interface, and enables unicast storm recovery for all interfaces. 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** 5

**Format** `storm-control unicast all rate`

**Mode** Global Config

*no storm-control unicast all rate*

This command returns the unicast storm recovery threshold to the default value and disables unicast storm recovery for all interfaces.

**Format** `no storm-control unicast all rate`

**Mode** Global Config

### **storm-control flowcontrol**

This command enables 802.3x flow control for the switch and only applies to full-duplex mode ports.



**Note:** 802.3x flow control works by pausing a port when the port becomes oversubscribed and dropping all traffic for small bursts of time during the congestion condition. This can lead to high-priority and/or network control traffic loss.

**Default** disabled

**Format** `storm-control flowcontrol`

**Mode** Global Config

*no storm-control flowcontrol*

This command disables 802.3x flow control for the switch.



**Note:** This command only applies to full-duplex mode ports.

**Format** `no storm-control flowcontrol`

**Mode** Global 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. Use the **a11** keyword to display the per-port configuration parameters for all interfaces, or specify the *slot/port* to display information about a specific interface.

**Format** `show storm-control [all | <slot/port>]`

**Mode** Privileged EXEC

Term	Definition
<b>Bcast Mode</b>	Shows whether the broadcast storm control mode is enabled or disabled.
<b>Bcast Level</b>	The broadcast storm control level.
<b>Mcast Mode</b>	Shows whether the multicast storm control mode is enabled or disabled.
<b>Mcast Level</b>	The multicast storm control level.
<b>Ucast Mode</b>	Shows whether the Unknown Unicast or DLF (Destination Lookup Failure) storm control mode is enabled or disabled.
<b>Ucast Level</b>	The Unknown Unicast or DLF (Destination Lookup Failure) storm control level.

## PORT-CHANNEL/LAG (802.3AD) COMMANDS

This section describes the commands you use to configure port-channels, which 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 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 slot/port number for the logical interface.



**Note:** Before you include a port in a port-channel, set the port physical mode. For more information, see [“This command disables a port. speed” on page 32.](#)

**Format**            `port-channel <name>`  
**Mode**             Global Config

*no port-channel*

This command deletes a port-channel (LAG).

**Format**            `no port-channel {<logical slot/port> | all}`  
**Mode**             Global Config

### addport

This command adds one port to the port-channel (LAG). The first interface is a logical slot/port number of a configured port-channel.



**Note:** Before adding a port to a port-channel, set the physical mode of the port. For more information, see [“This command disables a port. speed” on page 32.](#)

**Format**            `addport <logical slot/port>`  
**Mode**             Interface Config

### deleteport (Interface Config)

This command deletes the port from the port-channel (LAG). The interface is a logical slot/port number of a configured port-channel.

**Format**            `deleteport <logical slot/port>`  
**Mode**             Interface Config

**deleteport (Global Config)**

This command deletes all configured ports from the port-channel (LAG). The interface is a logical slot/port number of a configured port-channel. To clear the port channels, see [“clear port-channel” on page 16](#).

**Format**            `deleteport {<logical 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 only applicable to port-channel 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. The valid range of *<delay>* is 0-65535.

**Default**            0x8000  
**Format**            `lACP collector max delay <delay>`  
**Mode**             Interface Config



**Note:** This command is only applicable 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**

Use this command to configure the LACP actor admin parameters.

### **lacp actor admin key**

Use this command to configure the administrative value of the LACP actor admin key. 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 only applicable 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**

Use this command to configure the administrative value of actor state as transmitted by the Actor in LACPDU. The valid value range is 0x00-0xFF.

**Default** 0x07

**Format** `lacp actor admin state {individual|longtimeout|passive}`

**Mode** Interface Config



**Note:** This command is only applicable to physical interfaces.

*no lacp actor admin state*

Use this command to configure the default administrative values of actor state as transmitted by the Actor in LACPDUs.

**Format**        `no lacp actor admin state {individual|longtimeout|passive}`  
**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 only applicable 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 only applicable 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 only applicable 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 only applicable 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 port**

Use this command to configure LACP actor port priority key.

### **lacp actor port priority**

Use this command to configure the priority value assigned to the Aggregation Port. The valid range for *<priority>* is 0 to 255.

**Default**           0x80

**Format**            `lacp actor port priority <priority>`

**Mode**             Interface Config



**Note:** This command is only applicable 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 actor system priority**

Use this command to configure the priority value associated with the LACP Actor's SystemID. The range for *<priority>* is 0 to 255.

**Default**           0x80

**Format**        `lacp actor system priority <priority>`  
**Mode**            Interface Config



**Note:** This command is only applicable to physical interfaces.

*no lacp actor system priority*

Use this command to configure the priority value associated with the Actor's SystemID.

**Format**        `lacp actor system priority`  
**Mode**            Interface Config

### **lacp partner admin key**

Use this command to configure the administrative value of the Key for the protocol partner. The valid range for <key> is 0 to 65535.

**Default**        0x0  
**Format**        `lacp partner admin key <key>`  
**Mode**            Interface Config



**Note:** This command is only applicable to physical interfaces.

*no lacp partner admin key*

Use this command to configure the administrative value of the Key for the protocol partner.

**Format**        `no lacp partner admin key <key>`  
**Mode**            Interface Config

### **lacp partner admin state**

Use this command to configure the current administrative value of actor state for the protocol Partner. The valid value range is 0x00-0xFF.

**Default**        0x07  
**Format**        `lacp partner admin state {individual|longtimeout|passive}`  
**Mode**            Interface Config



**Note:** This command is only applicable to physical interfaces.

*no lacp partner admin state*

Use this command to configure the default current administrative value of actor state for the protocol partner.

**Format**            `no lacp partner admin state {individual|longtimeout|passive}`

**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 only applicable 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 only applicable 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 only applicable 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 only applicable 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. 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 only applicable to physical interfaces.

### *no lACP partner port id*

Use this command to set the LACP partner port id to the default.

**Format**            `lACP partner port-id`  
**Mode**             Interface Config

### lACP partner port priority

Use this command to configure the LACP partner port priority. The valid range for *<priority>* is 0 to 255.

**Default**            0x0  
**Format**            `lACP partner port priority <priority>`  
**Mode**             Interface Config



**Note:** This command is only applicable 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. 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 only applicable 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. The valid range for *<priority>* is 0 to 255.

**Default**            0x0

**Format**            `lacp partner system priority <priority>`

**Mode**             Interface Config



**Note:** This command is only applicable 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

**port-channel static**

This command enables the static mode on a port-channel (LAG) interface. By default the static mode for a new port-channel is disabled, which means the port-channel is dynamic. However if the maximum number of allowable dynamic port-channels are already present in the system, the static mode for a new port-channel enabled, which means the port-channel is static. You can only use this command on port-channel interfaces.

**Default**        disabled  
**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.

**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 all  
**Mode** Global Config

### no port lacpmode all

This command disables Link Aggregation Control Protocol (LACP) on all ports.

**Format** no port lacpmode all  
**Mode** Global Config

### port lacptimeout (Interface Config)

This command sets the timeout on a physical interface 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

### 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

**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

**port-channel adminmode**

This command enables a port-channel (LAG). The option **a11** sets every configured port-channel with the same administrative mode setting.

**Format**        `port-channel adminmode [all]`  
**Mode**         Global Config

*no port-channel adminmode*

This command disables a port-channel (LAG). The option **a11** sets every configured port-channel 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 slot/port for a configured port-channel. The option **a11** sets every configured port-channel with the same administrative mode setting.

**Default**        enabled  
**Format**        `port-channel linktrap {<logical 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 **a11** sets every configured port-channel with the same administrative mode setting.

**Format**        `no port-channel linktrap {<logical slot/port> | all}`  
**Mode**         Global Config

### port-channel name

This command defines a name for the port-channel (LAG). The interface is a logical slot/port for a configured port-channel, and *<name>* is an alphanumeric string up to 15 characters.

**Format** `port-channel name {<logical slot/port> | all | <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.

**Format** `show lacp actor {<slot/port>|all}`  
**Mode** Global Config

The following output parameters are displayed.

Parameter	Description
<b>System Priority</b>	The administrative value of the Key.
<b>Actor Admin Key</b>	The administrative value of the Key.
<b>Port Priority</b>	The priority value assigned to the Aggregation Port.
<b>Admin State</b>	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.

**Format** `show lacp actor {<slot/port>|all}`  
**Mode** Privileged EXEC

The following output parameters are displayed.

Parameter	Description
<b>System Priority</b>	The administrative value of priority associated with the Partner's System ID.
<b>System-ID</b>	The value representing the administrative value of the Aggregation Port's protocol Partner's System ID.
<b>Admin Key</b>	The administrative value of the Key for the protocol Partner.
<b>Port Priority</b>	The administrative value of the Key for protocol Partner.
<b>Port-ID</b>	The administrative value of the port number for the protocol Partner.
<b>Admin State</b>	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**
- Privileged EXEC
  - User EXEC

For each port-channel the following information is displayed:

Term	Definition
<b>Logical Interface</b>	The slot/port of the logical interface.
<b>Port-channel Name</b>	The name of port-channel (LAG) interface.
<b>Link-State</b>	Shows whether the link is up or down.
<b>Type</b>	Shows whether the port-channel is statically or dynamically maintained.
<b>LACP Device Type/Timeout</b>	The timeout ( <b>long</b> or <b>short</b> ) for the type of device ( <b>actor</b> or <b>partner</b> ).
<b>Mbr Ports</b>	The members of this port-channel.
<b>Active Ports</b>	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 {<logical slot/port> | all}`

- Mode**
- Privileged EXEC
  - User EXEC

Term	Definition
<b>Logical Interface</b>	Valid slot and port number separated by a forward slash.
<b>Port-Channel Name</b>	The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.
<b>Link State</b>	Indicates whether the Link is up or down.

Term	Definition
<b>Admin Mode</b>	May be enabled or disabled. The factory default is enabled.
<b>Mbr Ports</b>	A listing of the ports that are members of this port-channel (LAG), in slot/port notation. There can be a maximum of eight ports assigned to a given port-channel (LAG).
<b>Device Timeout</b>	For each port, lists the timeout ( <b>long</b> or <b>short</b> ) for Device Type ( <b>actor</b> or <b>partner</b> ).
<b>Port Speed</b>	Speed of the port-channel port.
<b>Type</b>	The status designating whether a particular port-channel (LAG) is statically or dynamically maintained. <ul style="list-style-type: none"> <li>• <b>Static</b> - The port-channel is statically maintained.</li> <li>• <b>Dynamic</b> - The port-channel is dynamically maintained.</li> </ul>
<b>Active Ports</b>	This field lists ports that are actively participating in the port-channel (LAG).

### show port-channel system priority

Use this command to display the port-channel system priority.

**Format** `show port-channel system priority`  
**Mode** Privileged EXEC

## PORT MIRRORING

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 <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 | tx}* option, the destination port monitors both ingress and egress packets. Use the *destination interface <slot/port>* to specify the interface to receive the monitored traffic. Use the *mode* parameter to enabled the administrative mode of the session. If enabled, the probe port monitors all the traffic received and transmitted on the physical monitored port.

**Format** `monitor session <session-id> {source interface <slot/port> [{rx | tx}] | destination interface <slot/port> | mode}`  
**Mode** Global Config

### 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 <slot/port>* parameter or *destination*

*interface <slot/port>* to remove the specified interface from the port monitoring session. Use the *mode* parameter to disable the administrative mode of the session.



**Note:** Since the current version of FL SWITCH GHS Firmware 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 <slot/port> | destination interface <slot/port> | mode}]`

**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
<b>Session ID</b>	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.
<b>Monitor Session Mode</b>	Indicates whether the Port Mirroring feature is enabled or disabled for the session identified with <i>&lt;session-id&gt;</i> . The possible values are Enabled and Disabled.
<b>Probe Port</b>	Probe port (destination port) for the session identified with <i>&lt;session-id&gt;</i> . If probe port is not set then this field is blank.
<b>Source Port</b>	The port, which is configured as mirrored port (source port) for the session identified with <i>&lt;session-id&gt;</i> . If no source port is configured for the session then this field is blank.
<b>Type</b>	Direction in which source port configured for port mirroring. Types are tx for transmitted packets and rx for receiving packets.

## IGMP SNOOPING CONFIGURATION COMMANDS

This section describes the commands you use to configure IGMP snooping. FL SWITCH GHS Firmware 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.

### set igmp

This command enables IGMP Snooping on the system (Global Config Mode) or an interface (Interface Config Mode). 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`  
**Mode**

- Global Config
- Interface Config

**Format** `set igmp <vlanid>`  
**Mode** VLAN Config

*no set igmp*

This command disables IGMP Snooping on the system, an interface or a VLAN.

**Format** `no set igmp`  
**Mode**

- Global Config
- Interface Config

**Format** `no set igmp <vlanid>`  
**Mode** VLAN Config

**set igmp groupmembership-interval**

This command sets the IGMP 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 IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds.

**Default** 260 seconds  
**Format** `set igmp groupmembership-interval <2-3600>`  
**Mode**

- Interface Config
- Global Config

**Format** `set igmp groupmembership-interval <vlan_id> <2-3600>`  
**Mode** 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`  
**Mode**

- Interface Config
- Global Config

**Format** `no set igmp groupmembership-interval <vlan_id>`  
**Mode** VLAN Config

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 mcrtexpiretime`  
**Mode**

- Global Config
- Interface Config

**show igmpsnooping**

This command displays IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled.

**Format** `show igmpsnooping [<slot/port> | <vlan_id>]`  
**Mode** Privileged EXEC

When the optional arguments *<slot/port>* or *<vlan\_id>* are not used, the command displays the following information:

Term	Definition
<b>Admin Mode</b>	Indicates whether or not IGMP Snooping is active on the switch.
<b>Multicast Control Frame Count</b>	The number of multicast control frames that are processed by the CPU.
<b>Interface Enabled for IGMP Snooping</b>	The list of interfaces on which IGMP Snooping is enabled.
<b>VLANS Enabled for IGMP Snooping</b>	The list of VLANS on which IGMP Snooping is enabled.

When you specify the *<slot/port>* values, the following information appears:

Term	Definition
<b>IGMP Snooping Admin Mode</b>	Indicates whether IGMP Snooping is active on the interface.
<b>Fast Leave Mode</b>	Indicates whether IGMP Snooping Fast-leave is active on the interface.
<b>Group Membership Interval</b>	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.
<b>Maximum Response Time</b>	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.
<b>Multicast Router Expiry Time</b>	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 appears:

Term	Definition
<b>VLAN ID</b>	The VLAN ID.
<b>IGMP Snooping Admin Mode</b>	Indicates whether IGMP Snooping is active on the VLAN.
<b>Fast Leave Mode</b>	Indicates whether IGMP Snooping Fast-leave is active on the VLAN.
<b>Group Membership Interval</b>	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.
<b>Maximum Response Time</b>	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.
<b>Multicast Router Expiry Time</b>	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.

### show igmpsnooping mrouter interface

This command displays information about statically configured ports.

**Format**            `show igmpsnooping mrouter interface <slot/port>`  
**Mode**              Privileged EXEC

Term	Definition
<b>Interface</b>	The port on which multicast router information is being displayed.
<b>Multicast Router Attached</b>	Indicates whether multicast router is statically enabled on the interface.
<b>VLAN ID</b>	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 <slot/port>`

**Mode** Privileged EXEC

Term	Definition
<b>Interface</b>	The port on which multicast router information is being displayed.
<b>VLAN ID</b>	The list of VLANs of which the interface is a member.

## 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.

### 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 ipv4_address]`  
**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 amount of time in seconds that the switch waits before sending another general query.

**Default** disabled  
**Format** `set igmp querier query-interval <1-18000>`  
**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 version**

Use this command to set the IGMP version of the query that the snooping switch is going to send 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

```

garp           Configure Generic Attribute Registration Protocol
                  parameters
gmrp          Set GARP Multicast Registration parameters
gvrp          Set GARP VLAN Registration Protocol parameters
igmp          Enable/Disable IGMP Snooping parameters

(Broadcom FASTPATH Switching) (Config)#set igmp?
<cr>           Press enter to execute the command
    
```

```
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 <vlanid>}]`  
**Mode**         Privileged EXEC

When the optional argument *<vlanid>* is not used, the command displays the following information.

Field	Description
<b>Admin Mode</b>	Indicates whether or not IGMP Snooping Querier is active on the switch.
<b>Admin Version</b>	The version of IGMP that will be used while sending out the queries.
<b>Querier Address</b>	The IP Address which will be used in the IPv4 header while sending out IGMP queries. It can be configured using the appropriate command.
<b>Query Interval</b>	The amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
<b>Querier Timeout</b>	The amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for *<vlanid>*, the following additional information appears.

Field	Description
<b>VLAN Admin Mode</b>	Indicates whether iGMP Snooping Querier is active on the VLAN.
<b>VLAN Operational State</b>	Indicates whether IGMP Snooping Querier is in “Querier” or “Non-Querier” state. When the switch is in <i>Querier</i> state, it will send out periodic general queries. When in <i>Non-Querier</i> state, it will wait for moving to Querier state and does not send out any queries.
<b>VLAN Operational Max Response Time</b>	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.
<b>Querier Election Participation</b>	Indicates whether the IGMP Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
<b>Querier VLAN Address</b>	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.
<b>Operational Version</b>	The version of IPv4 will be used while sending out IGMP queries on this VLAN.

## FL SWITCH GHS CLI

Field	Description
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
Last Querier Version	Indicates the IGMP version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument *detail* is used, the command shows the global information and the information for all Querier-enabled VLANs.

### show igmpsnooping

This command displays IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled.

**Format**            `show igmpsnooping [<slot/port> | <vlan_id>]`  
**Mode**             Privileged EXEC

When the optional arguments *<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 *<slot/port>* values, the following information appears:

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 appears:

Term	Definition
VLAN ID	The VLAN ID.

Term	Definition
<b>IGMP Snooping Admin Mode</b>	Indicates whether IGMP Snooping is active on the VLAN.
<b>Fast Leave Mode</b>	Indicates whether IGMP Snooping Fast-leave is active on the VLAN.
<b>Group Membership Interval</b>	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.
<b>Maximum Response Time</b>	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.
<b>Multicast Router Expiry Time</b>	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.

### show igmpsnooping mrouter interface

This command displays information about statically configured ports.

**Format** `show igmpsnooping mrouter interface <slot/port>`  
**Mode** Privileged EXEC

Term	Definition
<b>Interface</b>	The port on which multicast router information is being displayed.
<b>Multicast Router Attached</b>	Indicates whether multicast router is statically enabled on the interface.
<b>VLAN ID</b>	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 <slot/port>`  
**Mode** Privileged EXEC

Term	Definition
<b>Interface</b>	The port on which multicast router information is being displayed.
<b>VLAN ID</b>	The list of VLANs of which the interface is a member.

## 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 30](#).



**Note:** Care must be taken, if CLI was used to configure the feature, and other options are configured via WEB/SNMP. The WEB/SNMP configuration will automatically set and overwrite some options to provide the simple configuration way.

### **port-security**

This command enables port locking at the system level (Global Config) or port level (Interface Config).

**Default** disabled  
**Format** `port-security`  
**Mode**

- Global Config
- Interface Config

*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.

**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.

**Default** 5  
**Format** `port-security max-static <maxvalue>`  
**Mode** Interface Config

*no port-security max-static*

This command sets maximum number (max. number = 8) 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. 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.

**Format** `port-security mac-address move`  
**Mode** Interface Config

**show port-security**

This command displays the port-security settings. If you do not use a parameter, the command displays the settings for the entire system. Use the optional parameters to display the settings on a specific interface or on all interfaces.

**Format** `show port-security [{<slot/port> | all}]`  
**Mode** Privileged EXEC

Term	Definition
<b>Admin Mode</b>	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 appears:

Term	Definition
<b>Admin Mode</b>	Port Locking mode for the Interface.
<b>Dynamic Limit</b>	Maximum dynamically allocated MAC Addresses.
<b>Static Limit</b>	Maximum statically allocated MAC Addresses.
<b>Violation Trap Mode</b>	Whether violation traps are enabled.

### **show port-security dynamic**

This command displays the dynamically locked MAC addresses for the port.

**Format** `show port-security dynamic <slot/port>`

**Mode** Privileged EXEC

Term	Definition
<b>MAC Address</b>	MAC Address of dynamically locked MAC.

### **show port-security static**

This command displays the statically locked MAC addresses for port.

**Format** `show port-security static <slot/port>`

**Mode** Privileged EXEC

Term	Definition
<b>MAC Address</b>	MAC Address of statically locked MAC.

### **show port-security violation**

This command displays the source MAC address of the last packet discarded on a locked port.

**Format** `show port-security violation <slot/port>`

**Mode** Privileged EXEC

Term	Definition
<b>MAC Address</b>	MAC Address of discarded packet on 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.

**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.

**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 re-initialization, 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. Use *sys-name* to transmit the system name TLV. To configure the system name, see See “snmp-server” on page 27. 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 See “description” on page 32.

- 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.

- 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.

**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

**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
<b>Transmit Interval</b>	How frequently the system transmits local data LLDPDUs, in seconds.
<b>Transmit Hold Multiplier</b>	The multiplier on the transmit interval that sets the TTL in local data LLDPDUs.
<b>Re-initialization Delay</b>	The delay before re-initialization, in seconds.
<b>Notification Interval</b>	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 {<slot/port> | all}`  
**Mode**             Privileged Exec

Term	Definition
<b>Interface</b>	The interface in a slot/port format.
<b>Link</b>	Shows whether the link is up or down.
<b>Transmit</b>	Shows whether the interface transmits LLDPDUs.
<b>Receive</b>	Shows whether the interface receives LLDPDUs.
<b>Notify</b>	Shows whether the interface sends remote data change notifications.
<b>TLVs</b>	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).
<b>Mgmt</b>	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 {<slot/port> | all}`  
**Mode**             Privileged Exec

Term	Definition
<b>Last Update</b>	The amount of time since the last update to the remote table in days, hours, minutes, and seconds.
<b>Total Inserts</b>	Total number of inserts to the remote data table.
<b>Total Deletes</b>	Total number of deletes from the remote data table.
<b>Total Drops</b>	Total number of times the complete remote data received was not inserted due to insufficient resources.
<b>Total Ageouts</b>	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
<b>Interface</b>	The interface in slot/port format.
<b>Transmit Total</b>	Total number of LLDP packets transmitted on the port.
<b>Receive Total</b>	Total number of LLDP packets received on the port.
<b>Discards</b>	Total number of LLDP frames discarded on the port for any reason.
<b>Errors</b>	The number of invalid LLDP frames received on the port.
<b>Ageouts</b>	Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.
<b>TVL Discards</b>	The number of TLVs discarded.
<b>TVL Unknowns</b>	Total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.

### 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 {<slot/port> | all}`

**Mode** Privileged EXEC

Term	Definition
<b>Local Interface</b>	The interface that received the LLDPDU from the remote device.
<b>Chassis ID</b>	The ID of the remote device.
<b>Port ID</b>	The port number that transmitted the LLDPDU.
<b>System Name</b>	The system name of the remote device.

### 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 <slot/port>`

**Mode** Privileged EXEC

Term	Definition
<b>Local Interface</b>	The interface that received the LLDPDU from the remote device.
<b>Chassis ID Subtype</b>	The type of identification used in the Chassis ID field.
<b>Chassis ID</b>	The chassis of the remote device.
<b>Port ID Subtype</b>	The type of port on the remote device.
<b>Port ID</b>	The port number that transmitted the LLDPDU.

Term	Definition
<b>System Name</b>	The system name of the remote device.
<b>System Description</b>	Describes the remote system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
<b>Port Description</b>	Describes the port in an alpha-numeric format. The port description is configurable.
<b>System Capabilities Supported</b>	Indicates the primary function(s) of the device.
<b>System Capabilities Enabled</b>	Shows which of the supported system capabilities are enabled.
<b>Management Address</b>	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.
<b>Time To Live</b>	The amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.

### 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 {<slot/port> | all}`  
**Mode** Privileged EXEC

Term	Definition
<b>Interface</b>	The interface in a slot/port format.
<b>Port ID</b>	The port ID associated with this interface.
<b>Port Description</b>	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 <slot/port>`  
**Mode** Privileged EXEC

Term	Definition
<b>Interface</b>	The interface that sends the LLDPDU.
<b>Chassis ID Subtype</b>	The type of identification used in the Chassis ID field.
<b>Chassis ID</b>	The chassis of the local device.
<b>Port ID Subtype</b>	The type of port on the local device.
<b>Port ID</b>	The port number that transmitted the LLDPDU.
<b>System Name</b>	The system name of the local device.

Term	Definition
<b>System Description</b>	Describes the local system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
<b>Port Description</b>	Describes the port in an alpha-numeric format.
<b>System Capabilities Supported</b>	Indicates the primary function(s) of the device.
<b>System Capabilities Enabled</b>	Shows which of the supported system capabilities are enabled.
<b>Management Address</b>	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. By enabling MED, you will be effectively enabling the transmit and receive function of LLDP.

<b>Default</b>	disabled
<b>Format</b>	<code>lldp med</code>
<b>Mode</b>	Interface Config

*no lldp med*

Use this command to disable MED.

<b>Format</b>	<code>no lldp med</code>
<b>Mode</b>	Interface Config

### **lldp med confignotification**

Use this command to configure all the ports to send the topology change notification.

<b>Default</b>	disabled
<b>Format</b>	<code>lldp med confignotification</code>
<b>Mode</b>	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).

**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

Term	Definition
<b>capabilities</b>	Transmit the LLDP capabilities TLV.
<b>ex-pd</b>	Transmit the LLDP extended PD TLV.
<b>ex-pse</b>	Transmit the LLDP extended PSE TLV.
<b>inventory</b>	Transmit the LLDP inventory TLV.
<b>location</b>	Transmit the LLDP location TLV.
<b>network-policy</b>	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

**show lldp med**

Use this command to display a summary of the current LLDP MED configuration.

**Format**        `show lldp med`  
**Mode**         Privileged Exec

**Example:** The following shows example CLI display output for the command.

```
(FL SWITCH GHS Firmware Routing) #show lldp med
LLDP MED Global Configuration

Fast Start Repeat Count: 3
Device Class: Network Connectivity
```

```
(FL SWITCH GHS Firmware 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

**Example:** The following shows example CLI display output for the command.

```
(FL SWITCH GHS Firmware 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
```

```
(FL SWITCH GHS Firmware 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
```

```
(FL SWITCH GHS Firmware Routing) #
```

### show lldp med local-device detail

Use this command to display detailed information about the LLDP MED data that a specific interface transmits. <slot/port> indicates a specific physical interface.

**Format**        `show lldp med local-device detail <slot/port>`

**Mode**         Privileged EXEC

**Example:** The following shows example CLI display output for the command.

```
(FL SWITCH GHS Firmware 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 {<slot/port> | all}`

**Mode** Privileged EXEC

**Example:** The following shows example CLI display output for the command.

```
(FL SWITCH GHS Firmware Routing) #show lldp med remote-device all
```

```
LLDP MED Remote Device Summary
```

```
Local
Interface  Device Class
-----  -
1/0/8      Class I
1/0/9      Not Defined
1/0/10     Class II
1/0/11     Class III
1/0/12     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 <slot/port>`

**Mode** Privileged EXEC

**Example:** The following shows example CLI display output for the command.

```
(FL SWITCH GHS Firmware Routing) #show lldp med remote-device detail
1/0/8
```

```
Local Interface: 1/0/8
```

```
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

## 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 timeout in seconds. The *<seconds>* parameter must be within the range of 10 to 1,000,000 seconds.

**Default** 300  
**Format** `bridge aging-time <10-1,000,000>`  
**Mode** Global Config

*no bridge aging-time*

This command sets the forwarding database address aging timeout to the default value.

**Format** `no bridge aging-time`  
**Mode** Global Config

**show forwardingdb agetime**

This command displays the timeout for address aging. In an IVL system, the [fdbid | all] parameter is required.

**Default** all  
**Format** `show forwardingdb agetime [fdbid | all]`  
**Mode** Privileged EXEC

Term	Definition
<b>Forwarding DB ID</b>	Fdbid (Forwarding database ID) indicates the forwarding database whose aging timeout is to be shown. The all option is used to display the aging timeouts associated with all forwarding databases. This field displays the forwarding database ID in an IVL system.
<b>Age-time</b>	<ul style="list-style-type: none"> <li>In an IVL system, this parameter displays the address aging timeout for the associated forwarding database.</li> <li></li> </ul>



---

## STATIC MCAST CONFIGURATION

This command is creating or deleting a static multicast group.

### Static\_mcast create

<b>Default</b>	disable
<b>Format</b>	set static_mcast create <mac_addr>
<b>Mode</b>	Global Config

### Static\_mcast delete

<b>Default</b>	disable
<b>Format</b>	set static_mcast delete <mac_addr>
<b>Mode</b>	Global Config

This command is adding or removing ports to or from a group.

### add\_port

<b>Default</b>	disable
<b>Format</b>	set static_mcast add_port <mac_addr>
<b>Mode</b>	Interface Config

### rem\_port

<b>Default</b>	disable
<b>Format</b>	set static_mcast rem_port <mac_addr>
<b>Mode</b>	Interface Config

## SET IGMP

This command is defining if a unknown multicast will be forwarded to a querier.

### block-unknown-mcast

<b>Default</b>	disable
<b>Format</b>	set IGMP block-unknown-mcast
<b>Mode</b>	Global Config

### forward-unknown-mcast

<b>Default</b>	enable
<b>Format</b>	set IGMP forward-unknown-mcast
<b>Mode</b>	Global Config



# Section 3: Quality of Service (QoS) Commands

This chapter describes the Quality of Service (QoS) commands available in the FL SWITCH GHS Firmware CLI.



**Note:** 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 (CoS) 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. For more information about 802.1p priority, see [“Voice VLAN Commands” on page 47](#).

**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

**cos-queue min-bandwidth**

This command specifies the minimum transmission bandwidth guarantee for each interface queue. 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 strict**

This command activates the strict priority scheduler mode for each specified queue.

**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

**traffic-shape**

This command specifies the maximum transmission bandwidth limit for the interface as a whole. 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 *<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](#)

**Format**            `show classofservice dot1p-mapping [<slot/port>]`

**Mode**              Privileged EXEC

[page 47.](#)

The following information is repeated for each user priority.

Term	Definition
<b>User Priority</b>	The 802.1p user priority value.
<b>Traffic Class</b>	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
<b>IP DSCP</b>	The IP DSCP value.
<b>Traffic Class</b>	The traffic class internal queue identifier to which the IP DSCP value is mapped.

**show interfaces cos-queue**

This command displays the class-of-service queue configuration for the specified interface. The *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 [<slot/port>]`  
**Mode** Privileged EXEC

Term	Definition
<b>Queue Id</b>	An interface supports n queues numbered 0 to (n-1). The specific n value is platform dependent.
<b>Minimum Bandwidth</b>	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.
<b>Scheduler Type</b>	Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This is a configured value.
<b>Queue Management Type</b>	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
<b>Interface</b>	The slot/port of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.
<b>Interface Shaping Rate</b>	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.

## MAC ACCESS CONTROL LIST (ACL) COMMANDS

This section describes the commands you use to configure MAC 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.
- For the Broadcom 5630x platform, if you configure an IP ACL on an interface, you cannot configure a MAC ACL on the same interface.

### 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.

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}**

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.



**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 re-specified.



**Note:** An implicit 'deny all' MAC rule always terminates the access list.



**Note:** For BCM5630x and BCM5650x based systems, assign-queue, redirect, and mirror attributes are configurable for a deny rule, but they have no operational effect.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination 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.

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, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp. Each of these translates into its equivalent Ethertype value(s).

**Table 11: Ethertype Keyword and 4-digit Hexadecimal Value**

Ethertype Keyword	Corresponding Value
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5
ipv4	0x0800
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 *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), where n is the number of user configurable queues available for the hardware platform. The *assign-queue* parameter is valid only for a **permit** rule.

For the device, the *mirror* parameter allows the traffic matching this rule to be copied to the specified *<slot/port>*, while the *redirect* parameter allows the traffic matching this rule to be forwarded to the specified *<slot/port>*. The *assign-queue* and *redirect* parameters are only valid for a **permit** rule.



**Note:** The *mirror* and *redirect* parameters are not available on the Broadcom 5630x platform.



**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.

**Format**            *{deny|permit} {<srcmac> | any} {<dstmac> | any} [<ethertypekey> | <0x0600-0xFFFF>] [vlan {eq <0-4095>}] [cos <0-7>] [[log] [assign-queue <queue-id>]] [{mirror | redirect} <slot/port>]*

**Mode**             Mac-Access-List Config

**mac access-group**

This command either attaches a specific MAC Access Control List (ACL) identified by *<name>* to an interface, 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 is only valid 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.

**Format**            **mac access-group** *<name>* [*vlan <vlan-id>*] **in** [*sequence <1-4294967295>*]

- Modes**
- Global Config
  - Interface Config

*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>* [*vlan <vlan-id>*] **in**

- Modes**
- Global Config
  - Interface Config

**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 [*name*] parameter to identify a specific MAC ACL to display.

**Format**            **show mac access-lists** [*name*]

**Mode**              Privileged EXEC

Term	Definition
<b>Rule Number</b>	The ordered rule number identifier defined within the MAC ACL.
<b>Action</b>	The action associated with each rule. The possible values are Permit or Deny.
<b>Source MAC Address</b>	The source MAC address for this rule.

Term	Definition
<b>Destination MAC Address</b>	The destination MAC address for this rule.
<b>Ethertype</b>	The Ethertype keyword or custom value for this rule.
<b>VLAN ID</b>	The VLAN identifier value or range for this rule.
<b>COS</b>	The COS (802.1p) value for this rule.
<b>Log</b>	Displays when you enable logging for the rule.
<b>Assign Queue</b>	The queue identifier to which packets matching this rule are assigned.
<b>Mirror Interface</b>	On Broadcom 5650x platforms, the unit/slot/port to which packets matching this rule are copied.
<b>Redirect Interface</b>	On this device, the slot/port to which packets matching this rule are forwarded.

## IP ACCESS CONTROL LIST (ACL) COMMANDS

This section describes the commands you use to configure IP 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:

- FL SWITCH GHS Firmware software does not support IP ACL configuration for IP packet fragments.
- 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.
- On Broadcom 5630x platforms, 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 12](#) describes the parameters for the `access-list` command.

IP Standard ACL:

**Format**      `access-list <1-99> {deny | permit} {every | <srcip> <srcmask>} [log] [assign-queue <queue-id>] [{mirror | redirect} <unit/slot/port>]`

**Mode** Global Config

IP Extended ACL:

**Format** `access-list <100-199> {deny | permit} {every | {{icmp | igmp | ip | tcp | udp | <number>} <srcip> <srcmask>[{eq {<portkey> | <0-65535>}} <dstip> <dstmask> [{eq {<portkey>| <0-65535>}}] [precedence <precedence> | tos <tos> <tosmask> | dscp <dscp>] [log] [assign-queue <queue-id>] [{mirror | redirect} <unit/slot/port>}`

**Mode** Global Config

**Table 12: 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. <b>Note:</b> 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
{icmp   igmp   ip   tcp   udp   <number>}	Specifies the protocol to filter for an extended IP ACL rule.
<srcip> <srcmask>	Specifies a source IP address and source netmask for match condition of the IP ACL rule.
[{eq {<portkey>   <0-65535>}}]	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: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, and www. Each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range.
<dstip> <dstmask>	Specifies a destination IP address and netmask for match condition of the IP ACL rule.
[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 dscp, precedence, tos/tosmask.
[log]	Specifies that this rule is to be logged.
[assign-queue <queue-id>]	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
[{mirror   redirect} <slot/port>]	For this device, specifies the mirror or redirect interface which is the slot/port to which packets matching this rule are copied or forwarded, respectively. The mirror and redirect parameters are not available on this device.

*no access-list*

This command deletes an IP ACL that is identified by the parameter <accesslistnumber> from the system. The range for <accesslistnumber> 1-99 for standard access lists and 100-199 for extended access lists.

**Format** `no access-list <accesslistnumber>`

**Mode** Global Config

### **ip access-group**

This command either attaches a specific IP ACL identified by *<accesslistnumber>* to an interface or associates with a VLAN ID in a given direction.

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.

**Default** none

**Format** `ip access-group <accesslistnumber> [vlan <vlan-id>] in [sequence <1-4294967295>]`

**Modes**

- Interface Config
- Global Config

*no ip access-group*

This command removes a specified IP ACL from an interface.

**Default** none

**Format** `no ip access-group <accesslistnumber> [vlan <vlan-id>] in`

**Mode**

- Interface Config
- Global Config

### **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**

This command displays an IP ACL <accesslistnumber> is the number used to identify the IP ACL.

**Format**            `show ip access-lists <accesslistnumber>`

**Mode**             Privileged EXEC



**Note:** Only the access list fields that you configure are displayed.

Term	Definition
<b>Rule Number</b>	The number identifier for each rule that is defined for the IP ACL.
<b>Action</b>	The action associated with each rule. The possible values are Permit or Deny.
<b>Match All</b>	Indicates whether this access list applies to every packet. Possible values are True or False.
<b>Protocol</b>	The protocol to filter for this rule.
<b>Source IP Address</b>	The source IP address for this rule.
<b>Source IP Mask</b>	The source IP Mask for this rule.
<b>Source L4 Port Keyword</b>	The source port for this rule.
<b>Destination IP Address</b>	The destination IP address for this rule.
<b>Destination IP Mask</b>	The destination IP Mask for this rule.
<b>Destination L4 Port Keyword</b>	The destination port for this rule.
<b>IP DSCP</b>	The value specified for IP DSCP.
<b>IP Precedence</b>	The value specified IP Precedence.
<b>IP TOS</b>	The value specified for IP TOS.
<b>Log</b>	Displays when you enable logging for the rule.
<b>Assign Queue</b>	The queue identifier to which packets matching this rule are assigned.
<b>Mirror Interface</b>	The unit/slot/port to which packets matching this rule are copied.
<b>Redirect Interface</b>	The unit/slot/port to which packets matching this rule are forwarded.

**show access-lists**

This command displays IP ACLs and MAC access control lists information for a designated interface and direction.

**Format**            `show access-lists interface <slot/port> in`

**Mode**             Privileged EXEC

Term	Definition
<b>ACL Type</b>	Type of access list (IP or MAC).

<b>Term</b>	<b>Definition</b>
<b>ACL ID</b>	Access List name for a MAC access list or the numeric identifier for an IP access list.
<b>Sequence Number</b>	An optional sequence number may be specified to indicate the order of this access list relative to other 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 access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. Valid range is (1 to 4294967295).

---



## Section 4: Utility Commands

This chapter describes the utility commands available in the FL SWITCH GHS Firmware CLI.



**Note:** The commands in this chapter are in one of four functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Copy commands transfer or save configuration and informational files to and from the switch.
- Clear commands clear some or all of the settings to factory defaults.

### DUAL IMAGE COMMANDS

FL SWITCH GHS Firmware 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 supplied image file from the permanent storage. The image to be deleted must be a backup image. If this image is the active image, or if this image is activated, an error message displays.

**Format**            `delete {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.

**Format**            `boot system <image-file-name>`  
**Mode**             Privileged EXEC

#### show bootvar

This command displays the version information and the activation status for the current active and backup images. The command also displays any text description associated with an image. This command displays the switch activation status.

**Format**            `show bootvar`  
**Mode**             Privileged EXEC

### filedescr

This command associates a given text description with an image. Any existing description will be replaced.

**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.

**Format**        `update bootcode`  
**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

This command displays the contents of the IP stack's Address Resolution Protocol (ARP) table. The IP stack only learns ARP entries associated with the management interfaces - network or service ports. ARP entries associated with routing interfaces are not listed.

**Format**        `show arp switch`  
**Mode**         Privileged EXEC

Term	Definition
<b>IP Address</b>	IP address of the management interface or another device on the management network.
<b>MAC Address</b>	Hardware MAC address of that device.
<b>Interface</b>	For a service port the output is <i>Management</i> . For a network port, the output is the slot/port of the physical interface.

### 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 3](#).

**Format**        `show hardware`

**Mode** Privileged EXEC

### show version

This command displays inventory information for the switch.



**Note:** The **show version** command will replace the **show hardware** command in future releases of the software.

**Format** `show version`

**Mode** Privileged EXEC

Term	Definition
<b>Switch Description</b>	Text used to identify the product name of this switch.
<b>Machine Type</b>	The machine model as defined by the Vital Product Data.
<b>Machine Model</b>	The machine model as defined by the Vital Product Data
<b>Serial Number</b>	The unique box serial number for this switch.
<b>FRU Number</b>	The field replaceable unit number.
<b>Part Number</b>	Manufacturing part number.
<b>Maintenance Level</b>	Hardware changes that are significant to software.
<b>Manufacturer</b>	Manufacturer descriptor field.
<b>Burned in MAC Address</b>	Universally assigned network address.
<b>Software Version</b>	The release.version.revision number of the code currently running on the switch.
<b>Operating System</b>	The operating system currently running on the switch.
<b>Network Processing Device</b>	The type of the processor microcode.
<b>Additional Packages</b>	The additional packages incorporated into this system.

### 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 {<slot/port> | switchport}`

**Mode** Privileged EXEC

The display parameters, when the argument is *<slot/port>*, are as follows:

Parameters	Definition
<b>Packets Received Without Error</b>	The total number of packets (including broadcast packets and multicast packets) received by the processor.
<b>Packets Received With Error</b>	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
<b>Broadcast Packets Received</b>	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
<b>Packets Transmitted Without Error</b>	The total number of packets transmitted out of the interface.
<b>Transmit Packets Errors</b>	The number of outbound packets that could not be transmitted because of errors.
<b>Collisions Frames</b>	The best estimate of the total number of collisions on this Ethernet segment.
<b>Time Since Counters Last Cleared</b>	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
<b>Broadcast Packets Received</b>	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
<b>Packets Received With Error</b>	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
<b>Packets Transmitted Without Error</b>	The total number of packets transmitted out of the interface.
<b>Broadcast Packets Transmitted</b>	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.
<b>Transmit Packet Errors</b>	The number of outbound packets that could not be transmitted because of errors.
<b>Address Entries Currently In Use</b>	The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.
<b>VLAN Entries Currently In Use</b>	The number of VLAN entries presently occupying the VLAN table.
<b>Time Since Counters Last Cleared</b>	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

### 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 {<slot/port> | switchport}`  
**Mode**             Privileged EXEC

When you specify a value for *<slot/port>*, the command displays the following information.

Term	Definition
<b>Packets Received</b>	<ul style="list-style-type: none"> <li>• <b>Total Packets Received (Octets)</b> - 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.</li> <li>• <b>Packets Received 64 Octets</b> - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).</li> <li>• <b>Packets Received 65–127 Octets</b> - 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).</li> <li>• <b>Packets Received 128–255 Octets</b> - 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).</li> <li>• <b>Packets Received 256–511 Octets</b> - 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).</li> <li>• <b>Packets Received 512–1023 Octets</b> - 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).</li> <li>• <b>Packets Received 1024–1518 Octets</b> - 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).</li> <li>• <b>Packets Received &gt; 1522 Octets</b> - The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.</li> <li>• <b>Packets RX and TX 64 Octets</b> - The total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).</li> <li>• <b>Packets RX and TX 65–127 Octets</b> - 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).</li> <li>• <b>Packets RX and TX 128–255 Octets</b> - 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).</li> <li>• <b>Packets RX and TX 256–511 Octets</b> - 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).</li> <li>• <b>Packets RX and TX 512–1023 Octets</b> - 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).</li> <li>• <b>Packets RX and TX 1024–1518 Octets</b> - 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).</li> <li>• <b>Packets RX and TX 1519–1522 Octets</b> - The total number of packets (including bad packets) received and transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).</li> <li>• <b>Packets RX and TX 1523–2047 Octets</b> - 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.</li> <li>• <b>Packets RX and TX 2048–4095 Octets</b> - 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.</li> <li>• <b>Packets RX and TX 4096–9216 Octets</b> - 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.</li> </ul>

Term	Definition
<b>Packets Received Successfully</b>	<ul style="list-style-type: none"> <li>• <b>Total Packets Received Without Error</b> - The total number of packets received that were without errors.</li> <li>• <b>Unicast Packets Received</b> - The number of subnetwork-unicast packets delivered to a higher-layer protocol.</li> <li>• <b>Multicast Packets Received</b> - 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.</li> <li>• <b>Broadcast Packets Received</b> - The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.</li> </ul>
<b>Packets Received with MAC Errors</b>	<ul style="list-style-type: none"> <li>• <b>Total</b> - The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.</li> <li>• <b>Jabbers Received</b> - 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.</li> <li>• <b>Fragments/Undersize Received</b> - The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).</li> <li>• <b>Alignment Errors</b> - 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.</li> <li>• <b>Rx FCS Errors</b> - 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.</li> <li>• <b>Overruns</b> - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.</li> </ul>
<b>Received Packets Not Forwarded</b>	<ul style="list-style-type: none"> <li>• <b>Total</b> - A count of valid frames received which were discarded (in other words, filtered) by the forwarding process</li> <li>• <b>Local Traffic Frames</b> - The total number of frames dropped in the forwarding process because the destination address was located off of this port.</li> <li>• <b>802.3x Pause Frames Received</b> - 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.</li> <li>• <b>Unacceptable Frame Type</b> - The number of frames discarded from this port due to being an unacceptable frame type.</li> <li>• <b>Multicast Tree Viable Discards</b> - The number of frames discarded when a lookup in the multicast tree for a VLAN occurs while that tree is being modified.</li> <li>• <b>Reserved Address Discards</b> - The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system.</li> <li>• <b>Broadcast Storm Recovery</b> - The number of frames discarded that are destined for <code>FF:FF:FF:FF:FF:FF</code> when Broadcast Storm Recovery is enabled.</li> <li>• <b>CFI Discards</b> - The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format.</li> <li>• <b>Upstream Threshold</b> - The number of frames discarded due to lack of cell descriptors available for that packet's priority level.</li> </ul>

Term	Definition
<b>Packets Transmitted Octets</b>	<ul style="list-style-type: none"> <li>• <b>Total Bytes</b> - 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. -----</li> <li>• <b>Packets Transmitted 64 Octets</b> - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).</li> <li>• <b>Packets Transmitted 65-127 Octets</b> - 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).</li> <li>• <b>Packets Transmitted 128-255 Octets</b> - 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).</li> <li>• <b>Packets Transmitted 256-511 Octets</b> - 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).</li> <li>• <b>Packets Transmitted 512-1023 Octets</b> - 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).</li> <li>• <b>Packets Transmitted 1024-1518 Octets</b> - 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).</li> <li>• <b>Max Frame Size</b> - The maximum size of the Info (non-MAC) field that this port will receive or transmit.</li> </ul>
<b>Packets Transmitted Successfully</b>	<ul style="list-style-type: none"> <li>• <b>Total</b> - The number of frames that have been transmitted by this port to its segment.</li> <li>• <b>Unicast Packets Transmitted</b> - 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.</li> <li>• <b>Multicast Packets Transmitted</b> - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.</li> <li>• <b>Broadcast Packets Transmitted</b> - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.</li> </ul>
<b>Transmit Errors</b>	<ul style="list-style-type: none"> <li>• <b>Total Errors</b> - The sum of Single, Multiple, and Excessive Collisions.</li> <li>• <b>Tx FCS Errors</b> - 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.</li> <li>• <b>Oversized</b> - The total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec. at 10 Mb/s.</li> <li>• <b>Underrun Errors</b> - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.</li> </ul>
<b>Transmit Discards</b>	<ul style="list-style-type: none"> <li>• <b>Total Discards</b> - The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.</li> <li>• <b>Single Collision Frames</b> - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.</li> <li>• <b>Multiple Collision Frames</b> - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.</li> <li>• <b>Excessive Collisions</b> - A count of frames for which transmission on a particular interface fails due to excessive collisions.</li> <li>• <b>Port Membership Discards</b> - The number of frames discarded on egress for this port due to egress filtering being enabled.</li> </ul>

Term	Definition
<b>Protocol Statistics</b>	<ul style="list-style-type: none"> <li>• <b>802.3x Pause Frames Transmitted</b> - 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.</li> <li>• <b>GVRP PDUs Received</b> - The count of GVRP PDUs received in the GARP layer.</li> <li>• <b>GVRP PDUs Transmitted</b> - The count of GVRP PDUs transmitted from the GARP layer.</li> <li>• <b>GVRP Failed Registrations</b> - The number of times attempted GVRP registrations could not be completed.</li> <li>• <b>GMRP PDUs Received</b> - The count of GMRP PDU's received in the GARP layer.</li> <li>• <b>GMRP PDUs Transmitted</b> - The count of GMRP PDU's transmitted from the GARP layer.</li> <li>• <b>GMRP Failed Registrations</b> - The number of times attempted GMRP registrations could not be completed.</li> <li>• <b>STP BPDUs Transmitted</b> - Spanning Tree Protocol Bridge Protocol Data Units sent.</li> <li>• <b>STP BPDUs Received</b> - Spanning Tree Protocol Bridge Protocol Data Units received.</li> <li>• <b>RST BPDUs Transmitted</b> - Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.</li> <li>• <b>RSTP BPDUs Received</b> - Rapid Spanning Tree Protocol Bridge Protocol Data Units received.</li> <li>• <b>MSTP BPDUs Transmitted</b> - Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.</li> <li>• <b>MSTP BPDUs Received</b> - Multiple Spanning Tree Protocol Bridge Protocol Data Units received.</li> </ul>
<b>Dot1x Statistics</b>	<ul style="list-style-type: none"> <li>• <b>EAPOL Frames Received</b> - The number of valid EAPOL frames of any type that have been received by this authenticator.</li> <li>• <b>EAPOL Frames Transmitted</b> - The number of EAPOL frames of any type that have been transmitted by this authenticator.</li> </ul>
<b>Time Since Counters Last Cleared</b>	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 appears.

Term	Definition
<b>Octets Received</b>	The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
<b>Total Packets Received Without Error</b>	The total number of packets (including broadcast packets and multicast packets) received by the processor.
<b>Unicast Packets Received</b>	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
<b>Multicast Packets Received</b>	The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
<b>Broadcast Packets Received</b>	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
<b>Receive Packets Discarded</b>	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. A possible reason for discarding a packet could be to free up buffer space.
<b>Octets Transmitted</b>	The total number of octets transmitted out of the interface, including framing characters.
<b>Packets Transmitted without Errors</b>	The total number of packets transmitted out of the interface.

Term	Definition
<b>Unicast Packets Transmitted</b>	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.
<b>Multicast Packets Transmitted</b>	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
<b>Broadcast Packets Transmitted</b>	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
<b>Transmit Packets Discarded</b>	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.
<b>Most Address Entries Ever Used</b>	The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.
<b>Address Entries in Use</b>	The number of Learned and static entries in the Forwarding Database Address Table for this switch.
<b>Maximum VLAN Entries</b>	The maximum number of Virtual LANs (VLANs) allowed on this switch.
<b>Most VLAN Entries Ever Used</b>	The largest number of VLANs that have been active on this switch since the last reboot.
<b>Static VLAN Entries</b>	The number of presently active VLAN entries on this switch that have been created statically.
<b>Dynamic VLAN Entries</b>	The number of presently active VLAN entries on this switch that have been created by GVRP registration.
<b>VLAN Deletes</b>	The number of VLANs on this switch that have been created and then deleted since the last reboot.
<b>Time Since Counters Last Cleared</b>	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

### 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 <slot/port>* parameter to view MAC addresses on a specific interface. 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 <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. If you enter `vlan <vlan_id>`, only the Mac Address, Interface, and Status fields appear.

Term	Definition
<b>Mac Address</b>	A unicast 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 <code>01:23:45:67:89:AB</code> . In an IVL system the MAC address will be displayed as 8 bytes.
<b>Interface</b>	The port through which this address was learned.
<b>Interface Index</b>	This object indicates the ifIndex of the interface table entry associated with this port.
<b>Status</b>	The status of this entry. The meanings of the values are: <ul style="list-style-type: none"> <li>• <i>Static</i>—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.</li> <li>• <i>Learned</i>—The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use.</li> <li>• <i>Management</i>—The value of the corresponding instance (system MAC address) is also the value of an existing instance of <code>dot1dStaticAddress</code>. It is identified with interface <code>0/1</code>. and is currently used when enabling VLANs for routing.</li> <li>• <i>Self</i>—The value of the corresponding instance is the address of one of the switch's physical interfaces (the system's own MAC address).</li> <li>• <i>GMRP Learned</i>—The value of the corresponding was learned via GMRP and applies to Multicast.</li> <li>• <i>Other</i>—The value of the corresponding instance does not fall into one of the other categories.</li> </ul>

If you enter the `interface <slot/port>` parameter, in addition to the MAC Address and Status fields, the following field appears:

Term	Definition
<b>VLAN ID</b>	The VLAN on which the MAC address was learned.

The following information displays if you enter the `count` parameter:

Term	Definition
<b>Dynamic Address count</b>	Number of MAC addresses in the forwarding database that were automatically learned.
<b>Static Address (User-defined) count</b>	Number of MAC addresses in the forwarding database that were manually entered by a user.
<b>Total MAC Addresses in use</b>	Number of MAC addresses currently in the forwarding database.
<b>Total MAC Addresses available</b>	Number of MAC addresses the forwarding database can handle.

**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:** Show running-config 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 will only display 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.)

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 sysinfo

This command displays switch information.

**Format**            `show sysinfo`

**Mode**             Privileged EXEC

Term	Definition
<b>Switch Description</b>	Text used to identify this switch.
<b>System Name</b>	Name used to identify the switch. The factory default is blank. To configure the system name, see <a href="#">“snmp-server” on page 27</a> .

Term	Definition
<b>System Location</b>	Text used to identify the location of the switch. The factory default is blank. To configure the system location, see <a href="#">“snmp-server” on page 27</a> .
<b>System Contact</b>	Text used to identify a contact person for this switch. The factory default is blank. To configure the system location, see <a href="#">“snmp-server” on page 27</a> .
<b>System ObjectID</b>	The base object ID for the switch’s enterprise MIB.
<b>System Up Time</b>	The time in days, hours and minutes since the last switch reboot.
<b>MIBs Supported</b>	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:

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

**Format** `show tech-support`

**Mode** Privileged EXEC

### terminal length

Use this command to set the number of lines of output to be displayed on the screen, i.e. pagination, for the `show running-config` and `show running-config all` commands. The terminal length size is either zero or a number in the range of 5 to 48. After the user-configured number of lines is displayed in one page, the system prompts the user for `--More--` or `(q)uit`. Press `q` or `Q` to quit, or press any key to display the next set of `<5-48>` lines. The command `terminal length 0` disables pagination and, as a result, the output of the `show running-config` command is displayed immediately.

**Default** 24 lines per page

**Format** `terminal length <0|5-48>`

**Mode** Privileged EXEC

### *no terminal length*

Use this command to set the terminal length to the default value.

### show terminal length

Use this command to display the value of the user-configured terminal length size.

**Format**            `show terminal length`

**Mode**             Privileged EXEC

## LOGGING COMMANDS

### show logging buffered

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

**Format**            `show logging buffered`

**Mode**             Privileged EXEC

Term	Definition
<b>Buffered (In-Memory) Logging</b>	Shows whether the In-Memory log is enabled or disabled.
<b>Buffered Logging Wrapping Behavior</b>	The behavior of the In Memory log when faced with a log full situation.
<b>Buffered Log Count</b>	The count of valid entries in the buffered log.

## 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 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.

- Default**
- count: 3 probes
  - interval: 3 seconds
  - size: 0 bytes
  - port: 33434
  - maxTtl: 30 hops
  - maxFail: 5 probes
  - initTtl: 1 hop
  -

**Format** `traceroute <ipaddr/hostname> [initTtl <initTtl>] [maxTtl <maxTtl>]  
 [maxFail <maxFail>] [interval <interval>] [count <count>]  
 [port <port>] [size <size>]`

**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
<b>ipaddr   hostname</b>	The <i>ipaddr</i> value should be a valid IP address. The <i>hostname</i> value should be a valid hostname.
<b>initTtl</b>	Use <i>initTtl</i> 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.
<b>maxTtl</b>	Use <i>maxTtl</i> to specify the maximum TTL. Range is 1 to 255.
<b>maxFail</b>	Use <i>maxFail</i> to terminate the traceroute after failing to receive a response for this number of consecutive probes. Range is 0 to 255.
<b>interval</b>	Use <i>interval</i> to specify the time between probes, in seconds. Range is 1 to 60 seconds.
<b>count</b>	Use the optional <i>count</i> parameter to specify the number of probes to send for each TTL value. Range is 1 to 10 probes.
<b>port</b>	Use the optional <i>port</i> 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.
<b>size</b>	Use the optional <i>size</i> parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.

**Example:** The following are examples of the CLI command.

**Example:** traceroute Success:

```
(FL SWITCH GHS Firmware Routing) # 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
```

**Example:** traceroute Failure:

```
(FL SWITCH GHS Firmware Routing) # 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

### **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 `<slot/port>`, for all the ports, or for the entire switch based upon the argument.

**Format**        `clear counters {<slot/port> | all}`

**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 port-channel**

This command clears all port-channels (LAGs).

**Format**        `clear port-channel`

**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.

**Format**        `clear vlan`  
**Mode**         Privileged EXEC

### **enable passwd**

This command prompts you to change the Privileged EXEC password. Passwords are a maximum of 64 alphanumeric characters. The password is case sensitive.

**Format**        `enable passwd`  
**Mode**         Privileged EXEC

### **enable passwd encrypted <password>**

This command allows the administrator to transfer the enable password between devices without having to know the password. The *<password>* parameter must be exactly 128 hexadecimal characters.

**Format**        `enable passwd encrypted <password>`  
**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.

- Default**
- The default count is 1.
  - The default interval is 3 seconds.
  - The default size is 0 bytes.
- Format**      `ping <ipaddress/hostname> [count <count>] [interval <interval>] [size <size>]`
- 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
<b>count</b>	Use the <b>count</b> parameter to specify the number of ping packets (ICMP Echo requests) that are sent to the destination address specified by the <i>&lt;ip-address&gt;</i> field. The range for <i>&lt;count&gt;</i> is 1 to 15 requests.
<b>interval</b>	Use the <b>interval</b> parameter to specify the time between Echo Requests, in seconds. Range is 1 to 60 seconds.
<b>size</b>	Use the <b>size</b> parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.

**Example:** The following are examples of the CLI command.

**Example:** ping success:

```
(FL SWITCH GHS Firmware Routing) #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
```

**Example:** ping failure:

**In Case of Unreachable Destination:**

```
(FL SWITCH GHS Firmware Routing) # 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
```

#### In Case Of Request TimedOut:

```
(FL SWITCH GHS Firmware Routing) # 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
```

#### 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

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 (*image1* and *image2*) on the file system. Upload and download files from a server by using TFTP or Xmodem. SFTP and SCP are available as additional transfer methods if the software package supports secure management.

**Format**            `copy <source> <destination>`  
**Mode**             Privileged EXEC

Replace the *<source>* and *<destination>* parameters with the options in [Table 13](#). For the *<url>* source or destination, use one of the following values:

```
{xmodem |
tftp://<ipaddr|hostname>|<ip6address>/<filepath>/<filename>
| sftp|scp://<username>@<ipaddr>|<filepath>/<filename>}
```

For TFTP, SFTP and SCP, the *<ipaddr|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 username for logging into the remote server via SSH.



**Caution!** Remember to upload the existing FL SWITCH GHS Firmware.cfg file off the switch prior to loading a new release image in order to make a backup.

**Table 13: Copy Parameters**

Source	Destination	Description
<i>nvr</i> am:backup-config	<i>nvr</i> am:startup-config	Copies the backup configuration to the startup configuration.
<i>nvr</i> am:clibanner	<url>	Copies the CLI banner to a server.
<i>nvr</i> am:errorlog	<url>	Copies the error log file to a server.
<i>nvr</i> am:FL SWITCH GHS Firmware.cfg	<url>	Uploads the binary config file to a server.
<i>nvr</i> am:log	<url>	Copies the log file to a server.
<i>nvr</i> am:script <scriptname>	<url>	Copies a specified configuration script file to a server.
<i>nvr</i> am:startup-config	<i>nvr</i> am:backup-config	Copies the startup configuration to the backup configuration.
<i>nvr</i> am:startup-config	<url>	Copies the startup configuration to a server.
<i>nvr</i> am:traplog	<url>	Copies the trap log file to a server.
<i>system</i> :running-config	<i>nvr</i> am:startup-config	Saves the running configuration to nvr
<url>	<i>nvr</i> am:clibanner	Downloads the CLI banner to the system.
<url>	<i>nvr</i> am:FL SWITCH GHS Firmware.cfg	Downloads the binary config file to the system.
<url>	<i>nvr</i> am: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>	<i>nvr</i> am:sshkey-dsa	Downloads an SSH key file. For more information, see <a href="#">“Secure Shell (SSH) Commands” on page 9</a> .
<url>	<i>nvr</i> am:sshkey-rsa1	Downloads an SSH key file.
<url>	<i>nvr</i> am:sshkey-rsa2	Downloads an SSH key file.
<url>	<i>nvr</i> am:sslpem-dhweak	Downloads an HTTP secure-server certificate.
<url>	<i>nvr</i> am:sslpem-dhstrong	Downloads an HTTP secure-server certificate.
<url>	<i>nvr</i> am:sslpem-root	Downloads an HTTP secure-server certificate. For more information, see <a href="#">“Hypertext Transfer Protocol (HTTP) Commands” on page 12</a> .
<url>	<i>nvr</i> am:sslpem-server	Downloads an HTTP secure-server certificate.
<url>	<i>nvr</i> am:startup-config	Downloads the startup configuration file to the system.
<url>	<i>nvr</i> am:system-image	Downloads a code image to the system.
<url>	kernel	Downloads a code file by xmodem, zmodem, or TFTP.
<url>	{image1   image2}	Download an image from the remote server to either image.
{image1   image2}	<url>	Upload either image to the remote server.
image1	image2	Copy image1 to image2.
image2	image1	Copy image2 to image1.

## SIMPLE NETWORK TIME PROTOCOL (SNTP) COMMANDS

This section describes the commands you use to automatically configure the system time and date by using 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 16.

**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 from 1-65535.

**Default** 123  
**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 16.

**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 will set the poll timeout for SNTP unicast clients in seconds to a value from 1-30.

**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 will set the poll retry for SNTP unicast clients to a value from 0 to 10.

**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 multicast client poll-interval**

This command will set the poll interval for SNTP multicast clients in seconds as a power of two where *<poll-interval>* can be a value from 6 to 16.

**Default**        6  
**Format**        `sntp multicast client poll-interval <poll-interval>`  
**Mode**         Global Config

*no sntp multicast client poll-interval*

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

**Format**        `no sntp multicast client poll-interval`  
**Mode**         Global Config

**sntp server**

This command configures an SNTP server (a maximum of three). The optional priority can be a value of 1-3, the version a value of 1-4, and the port id a value of 1-65535.

**Format**        `sntp server <ipaddress/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/hostname>`  
**Mode**         Global Config

**show sntp**

This command is used to display SNTP settings and status.

**Format**        `show sntp`  
**Mode**         Privileged EXEC

Term	Definition
<b>Last Update Time</b>	Time of last clock update.
<b>Last Attempt Time</b>	Time of last transmit query (in unicast mode).
<b>Last Attempt Status</b>	Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).
<b>Broadcast Count</b>	Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.
<b>Multicast Count</b>	Current number of unsolicited multicast 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
<b>Client Supported Modes</b>	Supported SNTP Modes (Broadcast, Unicast, or Multicast).
<b>SNTP Version</b>	The highest SNTP version the client supports.
<b>Port</b>	SNTP Client Port.
<b>Client Mode</b>	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
<b>Server IP Address / Hostname</b>	IP address or hostname of configured SNTP Server.
<b>Server Type</b>	Address Type of Server.
<b>Server Stratum</b>	Claimed stratum of the server for the last received valid packet.
<b>Server Reference ID</b>	Reference clock identifier of the server for the last received valid packet.
<b>Server Mode</b>	SNTP Server mode.
<b>Server Maximum Entries</b>	Total number of SNTP Servers allowed.
<b>Server Current Entries</b>	Total number of SNTP configured.

For each configured server:

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



## Section 5: Management Commands

This chapter describes the management commands available in the FL SWITCH GHS Firmware CLI.

### NETWORK INTERFACE COMMANDS



**Caution!** 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.

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 48](#)

#### **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

#### **network parms**

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

**Format**            `network parms <ipaddr> <netmask> [<gateway>]`  
**Mode**             Privileged EXEC

#### **network protocol**

This command specifies the network configuration protocol to be used. If you modify this value, 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.

**Default**            `none`  
**Format**            `network protocol {none | bootp | dhcp}`

**Mode** Privileged EXEC

### 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.

**Format**            `show network`

- Modes**
- Privileged EXEC
  - User EXEC

Term	Definition
<b>IP Address</b>	The IP address of the interface. The factory default value is 0.0.0.0.
<b>Subnet Mask</b>	The IP subnet mask for this interface. The factory default value is 0.0.0.0.
<b>Default Gateway</b>	The default gateway for this IP interface. The factory default value is 0.0.0.0.

**Example:** The following shows example CLI display output for the network port.

```
(admin) #show network

IP Address..... 10.250.3.1
Subnet Mask..... 255.255.255.0
Default Gateway..... 10.250.3.3
Burned In MAC Address..... 00:10:18:82:03:37
Locally Administered MAC Address..... 00:00:00:00:00:00
MAC Address Type..... Burned In
Network Configuration Protocol Current..... None
Management VLAN ID..... 1
Web Mode..... Enable
Java Mode..... Enable
```

**Example:** The following shows example CLI display output for the service port.

## 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

### lineconfig

This command gives you access to the Line Config mode, which allows you to configure various Telnet settings and the console port.

**Format**            `lineconfig`  
**Mode**             Global Config

### 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

### **show serial**

This command displays serial communication settings for the switch.

**Format** `show serial`

**Modes**

- Privileged EXEC
- User EXEC

Term	Definition
<b>Serial Port Login Timeout (minutes)</b>	The time, in minutes, of inactivity on a Serial port connection, after which the Switch will close the connection. Any numeric value between 0 and 160 is allowed, the factory default is 5. A value of 0 disables the timeout.
<b>Baud Rate (bps)</b>	The default baud rate at which the serial port will try to connect. The available values are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 baud. The factory default is 9600 baud.
<b>Character Size (bits)</b>	The number of bits in a character. The number of bits is always 8.
<b>Flow Control</b>	Whether Hardware Flow-Control is enabled or disabled. Hardware Flow Control is always disabled.
<b>Stop Bits</b>	The number of Stop bits per character. The number of Stop bits is always 1.
<b>Parity Type</b>	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* value 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 *noecho* option disables local echo.

**Format** `telnet <ip-address/> <port> [debug] [line] [noecho]`

- 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. A value of 0 indicates that no outbound Telnet session can be established.

**Default**        5  
**Format**        `session-limit <0-5>`  
**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**

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

**Default**        5  
**Format**        `session-timeout <1-160>`  
**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. A value of 0 indicates that no Telnet connection can be established. The range is 0-5.

**Default** 5  
**Format** `telnetcon maxsessions <0-5>`  
**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 timeout value, in minutes. A session is active as long as the session has not been idle for the value set. The time is a decimal value from 1 to 160.



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

**Default** 5  
**Format** `telnetcon timeout <1-160>`  
**Mode** Privileged EXEC

*no telnetcon timeout*

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



**Note:** Changing the timeout value for active sessions does not become effective until the session is reaccessed. Also, any keystroke activates the new timeout 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.

<b>Format</b>	<code>show telnet</code>
<b>Modes</b>	<ul style="list-style-type: none"> <li>• Privileged EXEC</li> <li>• User EXEC</li> </ul>

Term	Definition
<b>Outbound Telnet Login Timeout</b>	The number of minutes an outbound Telnet session is allowed to remain inactive before being logged off.
<b>Maximum Number of Outbound Telnet Sessions</b>	The number of simultaneous outbound Telnet connections allowed.
<b>Allow New Outbound Telnet Sessions</b>	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.

<b>Format</b>	<code>show telnetcon</code>
<b>Modes</b>	<ul style="list-style-type: none"> <li>• Privileged EXEC</li> <li>• User EXEC</li> </ul>

Term	Definition
<b>Remote Connection Login Timeout (minutes)</b>	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.
<b>Maximum Number of Remote Connection Sessions</b>	This object indicates the number of simultaneous remote connection sessions allowed. The factory default is 5.
<b>Allow New Telnet Sessions</b>	New Telnet sessions will not be allowed when this field is set to no. The factory default value is yes.

**SECURE SHELL (SSH) COMMANDS**

This section describes the commands you use to configure 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** 1 and 2  
**Format** `ip ssh protocol [1] [2]`  
**Mode** Privileged EXEC

### **ip ssh server enable**

This command enables the IP secure shell server.

**Default** disabled  
**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. A value of 0 indicates that no ssh connection can be established. The range is 0 to 5.

**Default** 5  
**Format** `sshcon maxsessions <0-5>`  
**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 is a decimal value from 1 to 160.

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

**Default**        5

**Format**        `sshcon timeout <1-160>`

**Mode**         Privileged EXEC

*no sshcon timeout*

This command sets the SSH connection session timeout value, in minutes, to the default.

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new timeout 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
<b>Administrative Mode</b>	This field indicates whether the administrative mode of SSH is enabled or disabled.
<b>Protocol Level</b>	The protocol level may have the values of version 1, version 2 or both versions 1 and version 2.
<b>SSH Sessions Currently Active</b>	The number of SSH sessions currently active.
<b>Max SSH Sessions Allowed</b>	The maximum number of SSH sessions allowed.

Term	Definition
<b>SSH Timeout</b>	The SSH timeout value in minutes.
<b>Keys Present</b>	Indicates whether the SSH RSA and DSA key files are present on the device.
<b>Key Generation in Progress</b>	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.

## HYPERTEXT TRANSFER PROTOCOL (HTTP) COMMANDS

This section describes the commands you use to configure 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 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.

<b>Default</b>	enabled
<b>Format</b>	<code>ip http server</code>
<b>Mode</b>	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.

<b>Format</b>	<code>no ip http server</code>
<b>Mode</b>	Privileged EXEC

### **ip http secure-server**

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

<b>Default</b>	disabled
<b>Format</b>	<code>ip http secure-server</code>
<b>Mode</b>	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 timeout for un-secure HTTP sessions in hours. Configuring this value to zero will give an infinite hard-timeout. When this timeout expires, the user will be forced to re-authenticate. 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 <0-168>`

**Mode**         Privileged EXEC

*no ip http session hard-timeout*

This command restores the hard timeout 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 un-secure HTTP sessions. Zero is the configurable minimum.

**Default** 16  
**Format** `ip http session maxsessions <0-16>`  
**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 timeout for un-secure HTTP sessions in minutes. Configuring this value to zero will give an infinite soft-timeout. When this timeout expires the user will be forced to re-authenticate. This timer begins on initiation of the Web session and is re-started with each access to the switch.

**Default** 5  
**Format** `ip http session soft-timeout <0-60>`  
**Mode** Privileged EXEC

### *no ip http session soft-timeout*

This command resets the soft timeout 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 timeout for secure HTTP sessions in hours. When this timeout expires, the user is forced to re-authenticate. This timer begins on initiation of the Web session and is unaffected by the activity level of the connection. The secure-session hard-timeout can not be set to zero (infinite).

**Default** 24  
**Format** `ip http secure-session hard-timeout <1-168>`  
**Mode** Privileged EXEC

*no ip http secure-session hard-timeout*

This command resets the hard timeout 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. Zero is the configurable minimum.

**Default**        16  
**Format**        `ip http secure-session maxsessions <0-16>`  
**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 timeout for secure HTTP sessions in minutes. Configuring this value to zero will give an infinite soft-timeout. When this timeout expires, you are forced to re-authenticate. This timer begins on initiation of the Web session and is re-started with each access to the switch. The secure-session soft-timeout can not be set to zero (infinite).

**Default**        5  
**Format**        `ip http secure-session soft-timeout <1-60>`  
**Mode**         Privileged EXEC

*no ip http secure-session soft-timeout*

This command restores the soft timeout 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 1-65535 and the default is port 443.

**Default**        443

## FL SWITCH GHS CLI

---

**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
<b>HTTP Mode (Unsecure)</b>	The unsecure HTTP server administrative mode.
<b>Java Mode</b>	The java applet administrative mode which applies to both secure and un-secure web connections.
<b>Maximum Allowable HTTP Sessions</b>	The number of allowable un-secure http sessions.
<b>HTTP Session Hard Timeout</b>	The hard timeout for un-secure http sessions in hours.
<b>HTTP Session Soft Timeout</b>	The soft timeout for un-secure http sessions in minutes.
<b>HTTP Mode (Secure)</b>	The secure HTTP server administrative mode.
<b>Secure Port</b>	The secure HTTP server port number.
<b>Secure Protocol Level(s)</b>	The protocol level may have the values of SSL3, TSL1, or both SSL3 and TSL1.
<b>Maximum Allowable HTTPS Sessions</b>	The number of allowable secure http sessions.

Term	Definition
<b>HTTPS Session Hard Timeout</b>	The hard timeout for secure http sessions in hours.
<b>HTTPS Session Soft Timeout</b>	The soft timeout for secure http sessions in minutes.
<b>Certificate Present</b>	Indicates whether the secure-server certificate files are present on the device.
<b>Certificate Generation in Progress</b>	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 and serial port connections to the switch.

**Format**            **show loginsession**

**Mode**             Privileged EXEC

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

## USER ACCOUNT COMMANDS

This section describes the commands you use to add, manage, and delete system users. FL SWITCH GHS Firmware 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.

### users name

This command adds a new user account, if space permits. The account `<username>` can be up to eight characters in length. You can use alphanumeric characters as well as the dash ('-') and underscore ('\_'). You can define up to six user names.



**Note:** The `<username>` is not case sensitive when you add and delete users, and when the user logs in. However, when you use the `<username>` to set the user password, authentication, or encryption, you must enter the `<username>` in the same case you used when you added the user. To see the case of the `<username>`, enter the `show users` command.

**Format**            `users name <username>`

**Mode**             Global Config

### *no users name*

This command removes a user account.

**Format**            `no users name <username>`

**Mode**             Global Config



**Note:** You cannot delete the “admin” user account.

### users passwd

Use this command to change a password. Passwords are a maximum of 64 alphanumeric characters. If a user is authorized for authentication or encryption is enabled, the password length must be at least eight alphanumeric characters. The password is case sensitive. When you change a password, a prompt asks for the old password. If there is no password, press enter. You must enter the `<username>` in the same case you used when you added the user. To see the case of the `<username>`, enter the `show users` command.



**Note:** To specify a blank password in the configuration script, you must specify it as a space within quotes, for example, “ ”. For more information about creating configuration scripts, see [“Configuration Scripting Commands” on page 480](#).

**Default**            no password

**Format**        **users passwd** <username>  
**Mode**         Global Config

*no users passwd*

This command sets the password of an existing user to blank. When you change a password, a prompt asks for the old password. If there is no password, press enter.

**Format**        **no users passwd** <username>  
**Mode**         Global Config

**users passwd** <username> **encrypted** <password>

This command allows the administrator to transfer local user passwords between devices without having to know the passwords. The <password> parameter must be exactly 128 hexadecimal characters. The user represented by the <username> parameter must be a pre-existing local user.

**Format**        **users passwd** <username> **encrypted** <password>  
**Mode**         Global Config

**show users**

This command displays the configured user names and their settings. This command is only available for users with Read/Write privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

**Format**        **show users**  
**Mode**         Privileged EXEC

Term	Definition
<b>User Name</b>	The name the user enters to login using the serial port, Telnet or Web.
<b>Access Mode</b>	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. There can only be one Read/Write user and up to five Read Only users.
<b>SNMPv3 Access Mode</b>	The SNMPv3 Access Mode. If the value is set to <b>ReadWrite</b> , the SNMPv3 user is able to set and retrieve parameters on the system. If the value is set to <b>ReadOnly</b> , the SNMPv3 user is only able to retrieve parameter information. The SNMPv3 access mode may be different than the CLI and Web access mode.
<b>SNMPv3 Authentication</b>	The authentication protocol to be used for the specified login user.
<b>SNMPv3 Encryption</b>	The encryption protocol to be used for the specified login user.

### show users accounts

This command displays the local user status with respect to user account lockout and password aging.

**Format**            `show users accounts`  
**Mode**             Privileged EXEC

Term	Definition
<b>User Name</b>	The local user account's user name.
<b>Access Mode</b>	The user's access level (read-only or read/write).
<b>Lockout Status</b>	Indicates whether the user account is locked out (true or false).
<b>Password Expiration Date</b>	The current password expiration date in date format.

### passwords min-length

Use this command to enforce a minimum password length for local users. The value also applies to the enable password. The valid range is 8-64.

**Default**            8  
**Format**            `passwords min-length <8-64>`  
**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 shall be stored for each user account. When a local user changes his or her password, the user will not be able to reuse any password stored in password history. This ensures that users don't reuse their passwords often. The valid range is 0-10.

**Default**            0  
**Format**            `passwords history <0-10>`  
**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 will be prompted to change it before logging in again. The valid range is 1-365. The default is 0, or no aging.

**Default**      0  
**Format**      `passwords aging <1-365>`  
**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 re-activate a locked user account. Password lockout does not apply to logins from the serial console. The valid range is 1-5. The default is 0, or no lockout count enforced.

**Default**      0  
**Format**      `passwords lock-out <1-5>`  
**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

### 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`.

**Format**        `write memory`  
**Mode**         Privileged EXEC

## CONFIGURATION

### show memcard

Copy `system:running-config nvram:startup-config <description> <cr>` to save the current configuration with the given description.

The command “`copy system:running-config nvram:startup-config <description> <cr>`” would save the current configuration with the `<description>`.

An alternative command to copy is “write memory”, which has the same effect.

The CLI also provides the commands to upload or download the configuration files.

Download: `copy <url> nvram:startup-config`

Upload: `copy nvram:startup-config <url>`

The memory card can be cleared with the command “clear memcard”. Some Card information is displayed by using “show memcard” which results in the following output:

### Show Commands in Priviledged Exec Mode for SFP, POE, SCRJ, Temperature, DHCP Relay Agent, enhanced Port Information and Time:

`show sfp <slot/port>` // SFP Module information

`show sfp all`

`show poe <slot/port>` // PoE Module information

`show poe all`

`show scrj <slot/port>` // POF SCRJ Module information

`show scrj all`

`show port full <slot/port>` // Display full port information

`show port full all`

show temperature show device temperature

show time // show internal device clock state

show ip dhcp relay-agent // show DHCP Relay Agent information

show ip helper-address (slot/port) - also list the global server IP address if the port is enabled for the same

### **Config Commands in Privileged Exec Mode for time settings at Real Time Clock:**

time set <hour> <minute> <second> <year> <month> <day> // set internal device clock

### **Config Commands in Global Config Mode for SNTP and DHCP Relay Agent:**

sntp manycast address <ipaddress> // set SNTP Multicast Address (should be a broadcast address)

sntp client utc-offset <-12 - 12> // set the local time zone

service dhcp-relay-agent // enable DHCP Relay Agent

no service dhcp-relay-agent // disable DHCP Relay Agent

ip dhcp relay-agent server <ipaddr> // Configure DHCP server IP address

ip dhcp relay-agent remote-id ip-address // Set the DHCP remote ID option 82 to IP Address

ip dhcp relay-agent remote-id mac-address // Set the DHCP remote ID option 82 to MAC Address

### **Config Commands for POE and DHCP Relay Agent in Interface Config Mode:**

poe power enable // enable Power over Ethernet

no poe power enable // disable Power over Ethernet

poe current-limitation enable // enable Power over Ethernet current limitation

no poe current-limitation enable // disable Power over Ethernet current limitation

poe fault-monitoring enable // enable Power over Ethernet fault monitoring

no poe fault-monitoring enable // disable Power over Ethernet fault monitoring

ip dhcp relay-agent // enable Interface for DHCP Relay Agent

no ip dhcp relay-agent // disable Interface for DHCP Relay Agent

ip -> helper-address -> <ipAddress>// Set IP Helper Address

no ip -> helper-address// Disable IP Helper Address

### MRP Commands

(\*)IMPORTANT NOTE: The term "licence" should be avoided in UIs. Instead the term "functionality" should be used. This is because of legal issues with patent owners concerning MRP. So "licence present" should be avoided, "functionality available" should be used instead.

If the device has a CLI, the following commands are supported:

Global config mode

#### configure device role

"mrp mode client" - enable client functionality

"mrp mode manager" - enable manager functionality (if no Manager license available, an error message will appear)

"no mrp mode" - disable MRP

#### configure ring ports

"mrp ports <port1> <port2>"

<port1> and <port2> specify the physical slot identifier of the device

#### configure vlan ID used for MRP packets

"mrp vlanid <vlan>"

<vlan> have to be a vlan identifier already configured on the device

#### configure manager priority

"mrp manager-priority <priority>"

<priority> have to be a value between 0 and 65535

configure MRP domain name

"mrp domain-name <name>"

<name> has to be a text string up to 32 chars long

show configuration and current parameter of MRP

"show mrp"

will list the following objects

- domain name

- license state
  - device role
  - ring port number and status
  - VLAN ID
- ( only if device role Manager is selected)
- manager priority
  - ring state
  - number of ring status changes
  - timestamp of last ring status change

**Spanning Tree enhanced Commands:**

(no) spanning-tree large-tree-support

Format: (no) spanning-tree large-tree-support

Mode: Global Config

(no) spanning-tree fast-ring-detection

Format: (no) spanning-tree fast-ring-detection

Mode: Global Config

show spanning-tree fast-rings

Mode: Privileged EXEC, User EXEC

Ring-Number

Local Ring Ports A & B (port number)

Blocking Port of Ring Port & Mac

Status (OK, Ring Port A Failed, Broken)

## PROFINET

(no) OperatingMode\_Profinet (Global config level) ; setup the operating mode to Default or Profinet. After changing this mode, the device will execute the changes described in section "Operating Mode"; used for configuration file

- (no) alarm <alarmtype> (profinet config level) ; dis-/enable alarm configuration for system wide alarms; used for configuration file
- (no) profinet <alarmtype> (interface config level); dis-/enable alarm configuration for port based alarms; used for configuration file
- installDate <text> (profinet config level); specify installation date for IM2; used for configuration file
- description <text> (profinet config level); specify description text for IM3; used for configuration file
- signature <text> (profinet config level); specify signature for IM4; used for configuration file
- show profinet (global level); show current information about alarm configuration and connection status

The already existing CLI command "network protocol <mode>" is extended by the mode "dcp".

### Profinet Commands

Command	Additions	where	Description
operatingmode profinet	"no" cmd	config	De-/Activates the profinet mode
profinet alarm mrp	"no" cmd, Config-File	config/profinet	De-/Activates profinet alarm for MRP
profinet alarm power	"no" cmd, Config-File	config/profinet	De-/Activates profinet alarm for power supply
profinet alarm <port> link	"no" cmd, Config-File	config/profinet	De-/Activates profinet alarm for linkmonitoring on this port
profinet alarm <port > pofscrj	"no" cmd, Config-File	config/profinet	De-/Activates profinet alarm for pof scrj diagnostic on this port

### Digital Input CLI commands

The following CLI commands have been implemented for digital input handling:

- show digital\_input
- This command enables the user to investigate digital input status. It is available in privileged mode.

### Link Monitoring CLI commands

The following CLI commands have been implemented for link monitoring handling:

- in privileged mode:
- show link-monitoring"
- in interface configuration mode:
- "link-monitoring" (enable link monitoring for this interface)

- "no link-monitoring" (disable link monitoring for this interface)

### Alarm contact CLI commands

The following CLI commands have been implemented for alarm contact handling:

- `alarm_contact [global | link_monitoring | mrp_ring_fault | poe_fault | port_security | power_supply] [contact_1 | contact_2]`
- This command is available in privileged mode. This command enables one of the alarm contacts (depending on last parameter `contact_1` or `contact_2`) for a special mode where special modes depend on the 1st parameter:
- `global`: Alarm contact is enabled globally, i.e. all it is armed for any event that might be configured separately.
- `link_monitoring`: If the corresponding contact is enabled globally, it will open in case of link monitoring events.
- `mrp_ring_fault`: If the corresponding contact is enabled globally, it will open in case of mrp ring failure event (only on MRP master!).
- `poe_fault`: If the corresponding contact is enabled globally, it will open in case of PoE failure event (only on MRP master!).
- `port_security`: If the corresponding contact is enabled globally, it will open in case of an not allowed MAC address detected at a protected port.
- `power_supply`: If the corresponding contact is enabled globally, it will open in case of failure of one Power Supply (US1 or US2).

## SNMP COMMANDS

This section describes the commands you 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 `<name>`, `<loc>` and `<con>` is from 1 to 31 alphanumeric characters.

<b>Default</b>	none
<b>Format</b>	<code>snmp-server {sysname &lt;name&gt;   location &lt;loc&gt;   contact &lt;con&gt;}</code>
<b>Mode</b>	Global Config

### SMNP

The following command can be used to configure SNMP via CLI:  
global configuration mode:

```
snmp-server version <0 = none / 1=snmpv1_2 / 2 = snmpV3>
```

as previously stated SNMPV3 is only available on devices that support this feature.

**snmp-server community**

This command adds (and names) a new SNMP community. A community *<name>* is a name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of *<name>* can be up to 16 case-sensitive characters.



**Note:** Community names in the SNMP Community Table must be unique. When making multiple entries 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 removes this community name from the table. The *<name>* is the community name to 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 address is the associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that 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 address is the associated community SNMP packet sending address and is used along with the client IP address value

to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 255.255.255.255 will allow access from only one station, and will use that machine's IP address for the client IP address. A value of 0.0.0.0 will allow 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. The community name may be up to 16 alphanumeric characters.

**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 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 associated with this community cannot manage the switch until the Status is changed back to Enable.

**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 associated with this community cannot manage the switch until the Status is changed back to Enable.

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

### **snmp-server community ro**

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

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

### 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 sending of new violation traps designating when a packet with a disallowed MAC address is received on a locked port.



**Note:** For other port security commands, see [“Protected Ports Commands” on page 31](#).

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

### *no snmp-server enable traps violation*

This command disables the sending of new 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`

<b>Mode</b>	Global Config	
	PoE	PoE port fault status changed
	authFail	Authentication Failure
	coldStart	Cold Start
	configFault	Configuration not saved
	digitalInput_1	Status change digital input 1
	digitalInput_2	Status change digital input 2
	fwHealth	Firmware status changed
	linkDown	Link Down
	linkUp	Link Up
	mrpRingFail	MRP Ring Failure
	passWdAccess	Admin Passw Access
	pofScrj	POF SCRJ threshold reached
	portSecurity	Port Security Violation
	powerSupply	Power Supply
	rstpNewRoot	<R>STP New Root
	rstpRingFail	<R>STP Ring Failure
	rstpTopoChange	<R>STP Topology changed

### snmptrap

This command adds an SNMP trap receiver. The maximum length of *<name>* is 16 case-sensitive alphanumeric characters. The *<snmpversion>* is the version of SNMP. The version parameter options are snmpv1 or snmpv2. The SNMP trap address can be set using an IPv4 address format.

**Example:** The following shows an example of the CLI command.

```
(admin #) snmptrap mytrap ip6addr 3099::2
```



**Note:** The *<name>* parameter does not need to be unique, however; the *<name>* and *<ipaddr>* pair must be unique. Multiple entries can exist with the same *<name>*, as long as they are associated with a different *<ipaddr>*. 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 page39.”

<b>Default</b>	snmpv2
<b>Format</b>	<b>snmptrap</b> <i>&lt;name&gt;</i> <i>&lt;ipaddr&gt;</i> [ <i>snmpversion</i> <i>&lt;snmpversion&gt;</i> ]
<b>Mode</b>	Global Config

*no snmptrap*

This command deletes trap receivers for a community.

<b>Format</b>	<b>no snmptrap</b> <i>&lt;name&gt;</i> <i>&lt;ipaddr&gt;</i>
<b>Mode</b>	Global Config

### snmptrap ipaddr

This command assigns an IP address to a specified community name. The maximum length of name is 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

### show snmpcommunity

This command displays SNMP community information. Six communities are supported. You can add, change, or delete communities. The switch does not have to be reset for changes to take effect.

The SNMP agent of the switch complies with SNMP Versions 1, 2 or 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
<b>SNMP Community Name</b>	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.
<b>Client IP Address</b>	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.
<b>Client IP Mask</b>	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.
<b>Access Mode</b>	The access level for this community string.
<b>Status</b>	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
<b>SNMP Trap Name</b>	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.
<b>IP Address</b>	The IPv4 address to receive SNMP traps from this device.
<b>SNMP Version</b>	SNMPv2
<b>Mode</b>	The receiver's status (enabled or disabled).

**Example:** The following shows an example of the CLI command.

```
(admin) #show snmptrap

Community Name  IpAddress Snmp Version  Mode
Mytrap         0.0.0.0  SNMPv2        Enable show trapflags
```

### show trapflags

This command displays trap conditions. The command's display shows all the enabled OSPFv2 and OSPFv3 trapflags. Configure which traps the switch should 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. You do not have to reset the switch to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

**Format**            `show trapflags`

**Mode**             Privileged EXEC

Term	Definition
<b>Authentication Flag</b>	Can be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.
<b>Link Up/Down Flag</b>	Can be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.
<b>Multiple Users Flag</b>	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).
<b>Spanning Tree Flag</b>	Can be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps are sent.
<b>Broadcast Storm Flag</b>	Can be enabled or disabled. The factory default is enabled. Indicates whether broadcast storm traps are sent.
<b>ACL Traps</b>	May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps are sent.
<b>DVMRP Traps</b>	Can be enabled or disabled. The factory default is disabled. Indicates whether DVMRP traps are sent.
<b>OSPFv2 Traps</b>	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 <i>disabled</i> . Otherwise, the command shows all the enabled OSPF traps' information.
<b>OSPFv3 Traps</b>	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 <i>disabled</i> . Otherwise, the command shows all the enabled OSPFv3 traps' information.
<b>PIM Traps</b>	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**

Use this command to set the NAS-IP address for the radius server.

**Default**           Interface IP address that connects the switch to the radius server.  
**Format**           **radius server attribute 4 [ipaddr]**  
**Mode**             Global Config

Term	Definition
<b>ipaddr</b>	A valid IP address.

*no radius server attribute 4*

Use this command to reset the NAS-IP address for the radius server.

**Format**            `no radius server attribute 4`

**Mode**             Global Config

### radius server host

This command is used to configure the RADIUS authentication and accounting server. If you use the *<auth>* parameter, the command configures the IP address or hostname to use to connect to a RADIUS authentication server. You can configure up to 3 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. The *<port>* number range is 1 - 65535, with 1812 being the default value.



**Note:** To re-configure a RADIUS authentication server to use the default UDP *<port>*, set the *<port>* parameter to 1812.

If you use the *<acct>* token, the command configures the IP address or hostname 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 hostname 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>*. The *<port>* must be a value in the range 1 - 65535, with 1813 being the default.



**Note:** To re-configure a RADIUS accounting server to use the default UDP *<port>*, set the *<port>* parameter to 1813.

**Format**            `radius server host {auth | acct} <ipaddr/hostname> [<port>]`

**Mode**             Global Config

*no radius server host*

This command is used to remove the configured RADIUS authentication server or the RADIUS accounting server. 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/hostname>` parameter must match the IP address or hostname of the previously configured RADIUS authentication / accounting server.

**Format**      `no radius server host {auth | acct} <ipaddress/hostname>`  
**Mode**        Global Config

### radius server key

This command is used to configure the shared secret between the RADIUS client and the RADIUS accounting / authentication 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 show running config command's display, 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/hostname> [encrypted <encrypted-password>]`  
**Mode**        Global Config

**Example:** The following shows an example of the CLI command.

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

### radius server msgauth

This command enables the message authenticator attribute for a specified server.

**Format**      `radius server msgauth <ipaddr/hostname>`  
**Mode**        Global Config

*no radius server msgauth*

This command disables the message authenticator attribute for a specified server.

**Format**      `no radius server msgauth <ipaddr/hostname>`  
**Mode**        Global Config

**radius server primary**

This command is used to configure the primary RADIUS authentication server for this RADIUS client. The primary server handles RADIUS requests. The remaining configured servers are only used if the primary server cannot be reached. You can configure up to three servers on each client. Only one of these servers can be configured as the primary. If a primary server is already configured prior to this command being executed, the server specified by the IP address or hostname specified used in this command will become the new primary server. The IP address or hostname must match that of a previously configured RADIUS authentication server.

**Format**        `radius server primary <ipaddr/hostname>`  
**Mode**         Global Config

**radius server retransmit**

This command sets the maximum number of times a request packet is re-transmitted when no response is received from the RADIUS server. The retries value is an integer in the range of 1 to 15.

**Default**        4  
**Format**        `radius server retransmit <retries>`  
**Mode**         Global Config

*no radius server retransmit*

This command sets the maximum number of times a request packet is re-transmitted, to the default value.

**Format**        `no radius server retransmit`  
**Mode**         Global Config

**radius server timeout**

This command sets the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received. The timeout value is an integer in the range of 1 to 30.

**Default**        5  
**Format**        `radius server timeout <seconds>`  
**Mode**         Global Config

*no radius server timeout*

This command sets the timeout value to the default value.

**Format**        `no radius server timeout`

**Mode** Global Config

**show radius**

This command is used to display the various RADIUS configuration items for the switch as well as the configured RADIUS servers. If the optional token 'servers' is not included, the following RADIUS configuration items are displayed.

**Format** `show radius [servers]`

**Mode** Privileged EXEC

Term	Definition
<b>Primary Server IP Address or Hostname</b>	The configured server currently in use for authentication.
<b>Number of configured servers</b>	The number of configured authentication servers, including DNS configured server.
<b>Max number of retransmits</b>	The configured value of the maximum number of times a request packet is retransmitted.
<b>Timeout Duration</b>	The configured timeout value, in seconds, for request re-transmissions.
<b>Accounting Mode</b>	Yes or No.

If you use the `[servers]` keyword, the following information displays:

Term	Definition
<b>IP Address or Hostname</b>	IP address or hostname of the configured RADIUS server.
<b>Port</b>	The port in use by this server.
<b>Type</b>	Primary or secondary.
<b>Secret Configured</b>	Yes / No.
<b>Message Authenticator</b>	The message authenticator attribute for the selected server, which can be enables or disables.

**show radius accounting**

This command is used to display the configured RADIUS accounting mode, accounting server and the statistics for the configured accounting server.

**Format** `show radius accounting [statistics <ipaddr/hostname>]`

**Mode** Privileged EXEC

If you do not specify any parameters, then only the accounting mode and the RADIUS accounting server details are displayed.

Term	Definition
<b>Mode</b>	Enabled or disabled.
<b>IP Address / Hostname</b>	The configured IP address or hostname of the RADIUS accounting server.
<b>Port</b>	The port in use by the RADIUS accounting server.
<b>Secret Configured</b>	Yes or No.

If you use the optional *statistics <ipaddr/hostname>* parameter, the statistics for the configured RADIUS accounting server are displayed. The IP address parameter must match that of a previously configured RADIUS accounting server. The following information regarding the statistics of the RADIUS accounting server is displayed.

Term	Definition
<b>Accounting Server IP Address / Hostname</b>	IP address or hostname of the configured RADIUS accounting server.
<b>Round Trip Time</b>	The time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from the RADIUS accounting server.
<b>Requests</b>	The number of RADIUS Accounting-Request packets sent to this accounting server. This number does not include retransmissions.
<b>Retransmission</b>	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
<b>Responses</b>	The number of RADIUS packets received on the accounting port from this server.
<b>Malformed Responses</b>	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
<b>Bad Authenticators</b>	The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.
<b>Pending Requests</b>	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
<b>Timeouts</b>	The number of accounting timeouts to this server.
<b>Unknown Types</b>	The number of RADIUS packets of unknown types, which were received from this server on the accounting port.
<b>Packets Dropped</b>	The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

### show radius statistics

This command is used to display the statistics for RADIUS or configured server. To show the configured RADIUS server statistic, the IP address or hostname specified must match that of a previously configured RADIUS server. On execution, the following fields are displayed.

**Format**            `show radius statistics [<ipaddr/hostname>]`  
**Mode**              Privileged EXEC

If you do not specify the IP address, then only Invalid Server Address field is displayed. Otherwise other listed fields are displayed.

Term	Definition
<b>Invalid Server Addresses or Hostname</b>	The number of RADIUS Access-Response packets received from unknown addresses.
<b>Server IP Address/ Hostname</b>	IP address or hostname of the Server.
<b>Round Trip Time</b>	The time interval, in hundredths of a second, between the most recent Access-Reply, Access-Challenge and the Access-Request that matched it from the RADIUS authentication server.
<b>Access Requests</b>	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
<b>Access Retransmission</b>	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
<b>Access Accepts</b>	The number of RADIUS Access-Accept packets, including both valid and invalid packets, which were received from this server.
<b>Access Rejects</b>	The number of RADIUS Access-Reject packets, including both valid and invalid packets, which were received from this server.
<b>Access Challenges</b>	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, which were received from this server.
<b>Malformed Access Responses</b>	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.
<b>Bad Authenticators</b>	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
<b>Pending Requests</b>	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
<b>Timeouts</b>	The number of authentication timeouts to this server.
<b>Unknown Types</b>	The number of RADIUS packets of unknown types, which were received from this server on the authentication port.
<b>Packets Dropped</b>	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

## ROUTING COMMANDS

### VRRP

## VRRP 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. 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.

**Format**        `no ip vrrp <vrid> mode`  
**Mode**         Interface Config

**ip vrrp ip**

This command sets the virtual router IP address value for an 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. You can use the optional [*secondary*] parameter 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.

**Format**        `no ip vrrp <vrid> <ipaddress> secondary`  
**Mode**         Interface Config

**ip vrrp authentication**

This command sets the authorization details value for the virtual router configured on a specified interface. The parameter *{none | simple}* specifies the authorization type for virtual router configured on the specified interface. The parameter [*key*] is optional, it is only required when authorization type is 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.

**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. The parameter *<vrid>* is the virtual router ID, which is an integer 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.

**Format**            `no ip vrrp <vrid> preempt`  
**Mode**              Interface Config

**ip vrrp priority**

This command sets the priority of a router within a VRRP group. Higher values equal higher priority. The range is from 1 to 254. The parameter *<vrid>* is the virtual router ID, whose range is 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 <1-254>`  
**Mode**              Interface Config

*no ip vrrp priority*

This command sets the default priority value for the virtual router configured on a specified interface.

**Format**            `no ip vrrp <vrid> priority`  
**Mode**              Interface Config

**ip vrrp timers advertise**

This command sets the frequency, in seconds, that an interface on the specified virtual router sends a virtual router advertisement.

**Default** 1  
**Format** ip vrrp <vrid> timers advertise <1-255>  
**Mode** Interface Config

*no ip vrrp timers advertise*

This command sets the default virtual router advertisement value for an interface.

**Format** no ip vrrp <vrid> timers advertise  
**Mode** Interface Config

**show ip vrrp interface stats**

This command displays the statistical information about each virtual router configured on the switch.

**Format** show ip vrrp interface stats <slot/port> <vrid>  
**Modes**

- Privileged EXEC
- User EXEC

Term	Definition
<b>Uptime</b>	The time that the virtual router has been up, in days, hours, minutes and seconds.
<b>Protocol</b>	The protocol configured on the interface.
<b>State Transitioned to Master</b>	The total number of times virtual router state has changed to MASTER.
<b>Advertisement Received</b>	The total number of VRRP advertisements received by this virtual router.
<b>Advertisement Interval Errors</b>	The total number of VRRP advertisements received for which advertisement interval is different than the configured value for this virtual router.
<b>Authentication Failure</b>	The total number of VRRP packets received that don't pass the authentication check.
<b>IP TTL errors</b>	The total number of VRRP packets received by the virtual router with IP TTL (time to live) not equal to 255.
<b>Zero Priority Packets Received</b>	The total number of VRRP packets received by virtual router with a priority of '0'.
<b>Zero Priority Packets Sent</b>	The total number of VRRP packets sent by the virtual router with a priority of '0'.
<b>Invalid Type Packets Received</b>	The total number of VRRP packets received by the virtual router with invalid 'type' field.
<b>Address List Errors</b>	The total number of VRRP packets received for which address list does not match the locally configured list for the virtual router.

Term	Definition
<b>Invalid Authentication Type</b>	The total number of VRRP packets received with unknown authentication type.
<b>Authentication Type Mismatch</b>	The total number of VRRP advertisements received for which 'auth type' not equal to locally configured one for this virtual router.
<b>Packet Length Errors</b>	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
<b>VRRP Admin Mode</b>	The administrative mode for VRRP functionality on the switch.
<b>Router Checksum Errors</b>	The total number of VRRP packets received with an invalid VRRP checksum value.
<b>Router Version Errors</b>	The total number of VRRP packets received with Unknown or unsupported version number.
<b>Router VRID Errors</b>	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.

- Format**            `show ip vrrp interface <slot/port> <vrid>`
- Modes**            • Privileged EXEC  
                       • User EXEC

Term	Definition
<b>IP Address</b>	The configured IP address for the Virtual router.
<b>VMAC address</b>	The VMAC address of the specified router.
<b>Authentication type</b>	The authentication type for the specific virtual router.
<b>Priority</b>	The priority value for the specific virtual router.

Term	Definition
<b>Advertisement interval</b>	The advertisement interval for the specific virtual router.
<b>Pre-Empt Mode</b>	The preemption mode configured on the specified virtual router.
<b>Administrative Mode</b>	The status (Enable or Disable) of the specific router.
<b>State</b>	The state (Master/backup) of the virtual router.

### 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
<b>Interface</b>	Valid slot and port number separated by a forward slash.
<b>VRID</b>	The router ID of the virtual router.
<b>IP Address</b>	The virtual router IP address.
<b>Mode</b>	Indicates whether the virtual router is enabled or disabled.
<b>State</b>	The state (Master/backup) of the virtual router.

## OSPF

`ip ospf area`

Use this command to enable OSPFv2 and set the area ID of an interface. 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. 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.

**Default** actual interface bandwidth

**Format** `bandwidth <1-10000000>`

**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. The value of `<type>` is either `none`, `simple` or `encrypt`. The `<key>` is composed of standard displayable, non-control 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 may be up to 16 bytes. If the type is `encrypt` a `<keyid>` in the range of 0 and 255 must be specified. Unauthenticated interfaces do not need an authentication key or authentication key ID. There is no default value for this command.

**Format** `ip ospf authentication {none | {simple <key>} | {encrypt <key> <keyid>}}`

**Mode** Interface Config

*no ip ospf authentication*

This command sets the default OSPF Authentication Type for the specified interface.

**Format** `no ip ospf authentication`

**Mode** Interface Config

### ip ospf cost

This command configures the cost on an OSPF interface. The *<cost>* parameter has a range of 1 to 65535.

**Default** 10  
**Format** `ip ospf cost <1-65535>`  
**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 dead-interval

This command sets the OSPF dead interval for the specified interface. 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 (i.e. 4). Valid values range in seconds from 1 to 2147483647.



**Note:** Effective with FL SWITCH GHS Firmware 4.4.4 and later, valid values range in seconds from 1 to 65535.

**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. 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. Valid values 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 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 priority**

This command sets the OSPF priority for the specified router interface. The priority of 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 <0-255>`  
**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. 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. Valid values range from 0 to 3600 (1 hour).

**Default**        5

**Format**        `ip ospf retransmit-interval <0-3600>`

**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. 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. Valid values for *<seconds>* range from 1 to 3600 (1 hour).

**Default**        1

**Format**        `ip ospf transmit-delay <1-3600>`

**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

**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

**ip ospf area**

Use this command to enable OSPFv2 and set the area ID of an interface. 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

## IP ROUTING COMMANDS

This section describes the commands you use to enable and configure IP routing on the switch.

### routing

This command enables IPv4 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.”

**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 master switch.

**Format** `ip routing`  
**Mode** Global Config

*no ip routing*

This command disables the IP Router Admin Mode for the master switch.

**Format**        `no ip routing`

**Mode**         Global Config

**ip address**

This command configures an IP address on an interface. You can also use this command to configure one or more secondary IP addresses on the interface. The value for *<ipaddr>* is the IP address of the interface. The value for *<subnetmask>* is a 4-digit dotted-decimal number which represents the subnet mask of the interface. The subnet mask must have contiguous ones and be no longer than 30 bits, for example 255.255.255.0. This command adds the label IP address in `show ip interface`.

**Format**        `ip address <ipaddr> <subnetmask> [secondary]`

**Mode**         Interface Config

*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 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>` parameter, the next hop is deleted. If you use the `<preference>` value, the preference value of the static route is reset to its default.

**Format** `no ip route <ipaddr> <subnetmask> [{<nexthopip> [<preference>] | Null0}]`  
**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. 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 <1-255>`

**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. 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. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. FL SWITCH GHS Firmware software currently does not fragment IP packets.

- Packets forwarded in hardware ignore the IP MTU.
- Packets forwarded in software are dropped if they exceed the IP MTU of the outgoing interface.

Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack. The IP stack uses its default IP MTU and ignores the value set using the ip mtu command.

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 32.) must take into account the size of the Ethernet header.

**Default** 1500 bytes  
**Format** `ip mtu <68-1500>`  
**Mode** Interface Config

*no ip mtu*

This command resets the ip mtu to the default value.

**Format** `no ip mtu <mtu>`  
**Mode** Interface Config

### encapsulation

This command configures the link layer encapsulation type for the packet. 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 ip brief

This command displays all the summary information of the IP.

**Format** `show ip brief`  
**Modes**

- Privileged EXEC
- User EXEC

Term	Definition
<b>Default Time to Live</b>	The computed TTL (Time to Live) of forwarding a packet from the local router to the final destination.
<b>Routing Mode</b>	Shows whether the routing mode is enabled or disabled.
<b>IP Forwarding Mode</b>	Shows whether forwarding of IP frames is enabled or disabled. This is a configured value.
<b>Maximum Next Hops</b>	The maximum number of next hops the packet can travel.

**show ip interface**

This command displays all pertinent information about the IP interface.

**Format**            `show ip interface <slot/port>`

- Modes**
- Privileged EXEC
  - User EXEC

Term	Definition
<b>Primary IP Address</b>	The primary IP address and subnet masks for the interface. This value appears only if you configure it.
<b>Secondary IP Address</b>	One or more secondary IP addresses and subnet masks for the interface. This value appears only if you configure it.
<b>Routing Interface Status</b>	Determine the operational status of IPv4 routing Interface. The possible values are Up or Down.
<b>Routing Mode</b>	The administrative mode of router interface participation. The possible values are enable or disable. This value is configurable.
<b>Administrative Mode</b>	The administrative mode of the specified interface. The possible values of this field are enable or disable. This value is configurable.
<b>Routing Configuration</b>	Displays whether Routing Configuration is enabled or disabled on the system.
<b>Interface Configuration Status</b>	Displays whether the Interface Configuration is enabled or disabled on the system.
<b>Forward Net Directed Broadcasts</b>	Displays whether forwarding of network-directed broadcasts is enabled or disabled. This value is configurable.
<b>Proxy ARP</b>	Displays whether Proxy ARP is enabled or disabled on the system.
<b>Local Proxy ARP</b>	Displays whether Local Proxy ARP is enabled or disabled on the interface.
<b>Active State</b>	Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.
<b>Link Speed Data Rate</b>	An integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).
<b>MAC Address</b>	The burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.
<b>Encapsulation Type</b>	The encapsulation type for the specified interface. The types are: Ethernet or SNAP.
<b>IP MTU</b>	The maximum transmission unit (MTU) size of a frame, in bytes.
<b>Bandwidth</b>	Shows the bandwidth of the interface.

Example: show ip interface

```
(r2) #show ip interface 0/2
```

```
Routing Interface Status..... Down
Routing Mode..... Disable
Administrative Mode..... Enable
Forward Net Directed Broadcasts..... Disable
Active State..... Inactive
```

## FL SWITCH GHS CLI

---

```
Link Speed Data Rate..... Inactive
MAC Address..... 00:10:18:82:0C:68
Encapsulation Type..... Ethernet
IP MTU..... 1500
Bandwidth..... 100000 kbps
```

### show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router.

**Format**            `show ip interface brief`

**Modes**

- Privileged EXEC
- User EXEC

Term	Definition
<b>Interface</b>	Valid slot and port number separated by a forward slash.
<b>IP Address</b>	The IP address of the routing interface in 32-bit dotted decimal format.
<b>IP Mask</b>	The IP mask of the routing interface in 32-bit dotted decimal format.
<b>Netdir Bcast</b>	Indicates if IP forwards net-directed broadcasts on this interface. Possible values are Enable or Disable.
<b>MultiCast Fwd</b>	The multicast forwarding administrative mode on the interface. Possible values are Enable or Disable.

### 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 non-best routes. If you do not use the *all* parameter, the command only displays the best route.



**Note:** If you use the *connected* keyword for *<protocol>*, the *all* option is not available because there are no best or non-best connected routes.

**Format**            `show ip route [{<ip-address> [<protocol>] | {<ip-address> <mask> [longer-prefixes] [<protocol>] | <protocol>} [all] | all}]`

**Modes**

- Privileged EXEC
- User EXEC

Term	Definition
<b>Route Codes</b>	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, Interface
```

The columns for the routing table display the following information:

Term	Definition
<b>Code</b>	The codes for the routing protocols that created the routes.
<b>IP-Address/Mask</b>	The IP-Address and mask of the destination network corresponding to this route.
<b>Preference</b>	The administrative distance associated with this route. Routes with low values are preferred over routes with higher values.
<b>Metric</b>	The cost associated with this route.
<b>via Next-Hop</b>	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.
<b>Interface</b>	The outgoing router interface to use when forwarding traffic to the next destination. For reject routes, the next hop interface would be Null0 interface.

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.

**Example:** The following shows example CLI display output for the command.

```
(FL SWITCH GHS Firmware 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

C       1.1.1.0/24 [0/1] directly connected,    0/11
C       2.2.2.0/24 [0/1] directly connected,    0/1
S       7.0.0.0/8 [1/0] directly connected,    Null0
S       12.0.0.0/8 [5/0] directly connected,    Null0
S       23.0.0.0/8 [3/0] directly connected,    Null0
O IA   24.0.0.0/8 [110/0] directly connected,    Null0
O      24.1.1.0/24 [110/11] via 1.1.1.1,    0/11
```

### show ip route summary

Use this command to display the routing table summary. Use the optional *all* parameter to show the number of all routes, including best and non-best routes. To include only the number of best routes, do not use the optional parameter.

**Format**            `show ip route summary [all]`

- Modes**
- Privileged EXEC
  - User EXEC

Term	Definition
<b>Connected Routes</b>	The total number of connected routes in the routing table.
<b>Static Routes</b>	Total number of static routes in the routing table.
<b>RIP Routes</b>	Total number of routes installed by RIP protocol.
<b>BGP Routes</b>	Total number of routes installed by BGP protocol.
<b>OSPF Routes</b>	Total number of routes installed by OSPF protocol.
<b>Reject Routes</b>	Total number of reject routes installed by all protocols.
<b>Total Routes</b>	Total number of routes in the routing table.

**Example:** The following shows example CLI display output for the command.

```
(FL SWITCH GHS Firmware Routing) #show ip route summary
```

```

Connected Routes.....1
Static Routes.....7
RIP Routes.....0
BGP Routes.....0
OSPF Routes.....0
  Intra Area Routes.....0
  Inter Area Routes.....0
  External Type-1 Routes.....0
  External Type-2 Routes.....0
Reject Routes.....2
Total routes.....8

```

### show ip route preferences

This command displays detailed information about the route preferences. 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
<b>Local</b>	The local route preference value.
<b>Static</b>	The static route preference value.
<b>OSPF Intra</b>	The OSPF Intra route preference value.
<b>OSPF Inter</b>	The OSPF Inter route preference value.
<b>OSPF External</b>	The OSPF External route preference value.
<b>RIP</b>	The RIP route preference value.
<b>BGP4</b>	The BGP-4 route preference value.

### **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

## **ROUTING INFORMATION PROTOCOL (RIP) COMMANDS**

This section describes the commands you use to view and configure RIP, which is a distance-vector routing protocol that you use to route traffic within a small network.

### **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.

- 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.

**Format**      `default-metric <0-15>`  
**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.

**Default**        15  
**Format**        `distance rip <1-255>`  
**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.

**Default**        0  
**Format**        `distribute-list <1-199> 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.

**Format**        `no distribute-list <1-199> 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 specified interface. The value of *<type>* is either *none*, *simple*, or *encrypt*. The value for authentication key [*key*] must be 16 bytes or less. The [*key*] is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. If the value of

*<type>* is *encrypt*, a keyid in the range of 0 and 255 must be specified. Unauthenticated interfaces do not need an authentication key or authentication key ID.

**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 the interface to allow RIP control packets of the specified version(s) to be received.

The value for *<mode>* is one of: *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 the interface to allow RIP control packets of the specified version to be sent. The value for *<mode>* is one of: *rip1* to broadcast RIP version 1 formatted packets, *rip1c* (RIP version 1 compatibility mode) which sends RIP version 2 formatted packets via broadcast, *rip2* for sending RIP version 2 using multicast, or *none* to not allow any RIP control packets to be sent.

**Default** ripi2  
**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 for this case. Simple - a route will not be included in updates sent to the router from which it was learned. Poisoned reverse - a route will be included in updates sent to the router from which it was learned, but the metric will be 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/routers. There are five possible match options. When you submit the command

redistribute ospf match <match-type> the match-type or types specified are added to any match types presently being redistributed. Internal routes are redistributed by default.

- Default**
- metric—not-configured
  - match—internal
- Format for OSPF as source protocol**     `redistribute ospf [metric <0-15>] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]`
- Format for other source protocol**     `redistribute {bgp | static | connected} [metric <0-15>]`
- Mode**     Router RIP Config

*no redistribute*

This command de-configures RIP protocol to redistribute routes from the specified source protocol/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
<b>RIP Admin Mode</b>	Enable or disable.
<b>Split Horizon Mode</b>	None, simple or poison reverse.
<b>Auto Summary Mode</b>	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.
<b>Host Routes Accept Mode</b>	Enable or disable. If enabled the router accepts host routes. The default is enable.
<b>Global Route Changes</b>	The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.
<b>Global queries</b>	The number of responses sent to RIP queries from other systems.
<b>Default Metric</b>	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.
<b>Default Route Advertise</b>	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 (i.e., ip rip).

**Format**            `show ip rip interface brief`

- Modes**
- Privileged EXEC
  - User EXEC

Term	Definition
<b>Interface</b>	Valid slot and port number separated by a forward slash.
<b>IP Address</b>	The IP source address used by the specified RIP interface.
<b>Send Version</b>	The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2
<b>Receive Version</b>	The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both
<b>RIP Mode</b>	The administrative mode of router RIP operation (enabled or disabled).
<b>Link State</b>	The mode of the interface (up or down).

### show ip rip interface

This command displays information related to a particular RIP interface.

**Format**            `show ip rip interface <slot/port>`

- Modes**
- Privileged EXEC
  - User EXEC

Term	Definition
<b>Interface</b>	Valid slot and port number separated by a forward slash. This is a configured value.
<b>IP Address</b>	The IP source address used by the specified RIP interface. This is a configured value.
<b>Send Version</b>	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.
<b>Receive Version</b>	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.
<b>Both RIP Admin Mode</b>	RIP administrative mode of router RIP operation; enable activates, disable de-activates it. This is a configured value.
<b>Link State</b>	Indicates whether the RIP interface is up or down. This is a configured value.
<b>Authentication Type</b>	The RIP Authentication Type for the specified interface. The types are none, simple, and encrypt. This is a configured value.
<b>Default Metric</b>	A number which represents the metric used for default routes in RIP updates originated on the specified interface. This is a configured value.

The following information will be invalid if the link state is down.

Term	Definition
<b>Bad Packets Received</b>	The number of RIP response packets received by the RIP process which were subsequently discarded for any reason.

Term	Definition
<b>Bad Routes Received</b>	The number of routes contained in valid RIP packets that were ignored for any reason.
<b>Updates Sent</b>	The number of triggered RIP updates actually sent on this interface.

## 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 11](#)) to capture the running configuration into a script. Use the `copy` command (see [“copy” on page 19](#)) to transfer the configuration script to or from the switch.

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:

- 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!
```



**Note:** 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>* parameter 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>* parameter 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** Global Config

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

### script show

This command displays the contents of a script file, which is named *<scriptname>*.

**Format** `script show <scriptname>`

**Mode** Privileged EXEC

---

Term	Definition
------	------------

<b>Output Format</b>	<code>line &lt;number&gt;: &lt;line contents&gt;</code>
----------------------	---

---

### **script validate**

This command validates a script file by parsing each line in the script file where `<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

