



# **KGS-2422-TG**

**Industrial Command Line Interface**

**(ICLI)**

**for console & Telnet**

**Operation Manual**



DOC.190530

(C) 2019 KTI Networks Inc. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation or transformation) without permission from KTI Networks Inc.

KTI Networks Inc. reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of KTI Networks Inc. to provide notification of such revision or change.

For more information, contact:

**United States**      KTI Networks Inc.  
P.O. BOX 631008  
Houston, Texas 77263-1008  
  
Phone: 713-2663891  
Fax: 713-2663893  
E-mail: [kti@ktinet.com](mailto:kti@ktinet.com)  
URL: <http://www.ktinet.com/>

**International**      Fax: 886-2-26983873  
E-mail: [kti@ktinet.com.tw](mailto:kti@ktinet.com.tw)  
URL: <http://www.ktinet.com.tw/>

The information contained in this document is subject to change without prior notice.  
Copyright (C) All Rights Reserved.

## **TRADEMARKS**

Ethernet is a registered trademark of Xerox Corp.

# Table of Contents

<b>1. Introduction.....</b>	<b>9</b>
1.1 Command Modes.....	9
1.2 Getting Help.....	9
1.3 Finding Command Options.....	10
1.4 Ethernet Interface Naming.....	11
<b>2. Terminal Editing .....</b>	<b>12</b>
2.1 Using the Keyboard.....	12
2.2 Basic Line Editing Keys.....	12
2.3 Command History Keys.....	12
2.4 Context-sensitive Help Keys.....	13
2.5 Pagination Control Keys.....	13
2.6 Other Special Keys.....	13
2.7 Terminal Parameters.....	14
2.8 Using Banner .....	14
<b>3. Working with Configuration Files .....</b>	<b>15</b>
3.1 Reverting to Default Configuration.....	15
<b>4. Working with Software Images .....</b>	<b>16</b>
<b>5. Commands in EXEC Mode .....</b>	<b>16</b>
5.1 clear Command.....	17
5.2 cls command.....	19
5.3 configure Command.....	19
5.4 copy Command.....	19
5.5 debug Command.....	20
5.6 delete Command.....	20
5.7 dir Command.....	20
5.8 do Command.....	21
5.9 dot1x Command.....	21
5.10 enable Command.....	21
5.11 exit Command.....	22

5.12 firmware Command .....	22
5.13 help Command.....	23
5.14 ip Command.....	23
5.15 ipv6 Command.....	24
5.16 logout Command.....	24
5.17 more Command .....	24
5.18 no Command.....	25
5.19 ping Command.....	25
5.20 platform Command.....	26
5.21 reload Command.....	26
5.22 send Command.....	27
5.23 show Command .....	27
5.24 terminal Command .....	33
5.25 veriphy Command .....	34
<b>6. Global Configuration Commands .....</b>	<b>35</b>
6.1 aaa command .....	36
6.2 access command .....	37
6.3 access-list Command .....	38
6.4 aggregation Command.....	39
6.5 banner Command .....	39
6.6 clock Command .....	39
6.7 default Command.....	40
6.8 do Command.....	40
6.9 dot1x Command.....	40
6.10 enable Command.....	42
6.11 end Command.....	42
6.12 exit Command.....	42
6.13 gvrp Command.....	43
6.14 help Command.....	43
6.15 hostname Command .....	43
6.16 interface Command.....	44
6.17 ip Commands .....	44

6.18 ip arp Command.....	45
6.19 ip dhcp Command .....	46
6.20 ip dns Command .....	46
6.21 ip domans Command .....	47
6.22 ip helper-address Command .....	47
6.23 ip http Command.....	47
6.24 ip igmp Command .....	48
6.25 ip name-server Command .....	48
6.26 ip route Command.....	49
6.27 ip routing Command .....	49
6.28 ip source Command .....	49
6.29 ip ssh.....	50
6.30 ip verify source Command.....	50
6.31 ipmc Command .....	50
6.32 ipv6 Command.....	51
6.33 json Command .....	52
6.34 lacp Command.....	52
6.35 line Command .....	52
6.36 lldp Command.....	53
6.37 logging Command .....	54
6.38 loop-protect Command.....	54
6.39 mac address-table Command.....	55
6.40 monitor Command.....	55
6.41 mvr Command.....	56
6.42 no Command.....	57
6.43 ntp Command.....	59
6.44 port-security Command .....	59
6.45 privilege Command .....	59
6.46 qos Command.....	60
6.47 radius-server Command.....	63
6.48 rmon Command .....	64
6.49 sflow Command .....	66

6.50 snmp-server Command.....	66
6.51 spanning-tree Command.....	68
6.52 tacacs-server Command .....	70
6.53 udld Command.....	70
6.54 upnp Command.....	71
6.55 username Command.....	71
6.56 vlan Command .....	72
6.57 voice Command .....	73
6.58 web Command.....	74
<b>7. Port Interface Configuration Commands .....</b>	<b>75</b>
7.1 Port Interface Configuration.....	75
7.2 (config-if)# access-list.....	76
7.3 (config-if)# aggregation .....	77
7.4 (config-if)# do .....	77
7.5 (config-if)# dot1x .....	78
7.6 (config-if)# duplex.....	78
7.7 (config-if)# end .....	79
7.8 (config-if)# excessive-restart .....	79
7.9 (config-if)# exit.....	79
7.10 (config-if)# flowcontrol .....	79
7.11 (config-if)# frame-length-check.....	79
7.12 (config-if)# green-ethernet .....	80
7.13 (config-if)# gvrp .....	80
7.14 (config-if)# help .....	80
7.15 (config-if)# ip .....	81
7.16 (config-if)# ipv6 mld .....	81
7.17 (config-if)# lacp.....	82
7.18 (config-if)# lldp.....	83
7.19 (config-if)# loop-protect .....	84
7.20 (config-if)# mac .....	84
7.21 (config-if)# media-type.....	84
7.22 (config-if)# mtu .....	85

7.23 (config-if)# mvr .....	85
7.24 (config-if)# no .....	86
7.25 (config-if)# platform .....	90
7.26 (config-if)# port-security.....	90
7.27 (config-if)# priority-flowcontrol.....	91
7.28 (config-if)# pvlan.....	91
7.29 (config-if)# qos .....	91
7.30 (config-if)# rmon .....	93
7.31 (config-if)# sflow .....	94
7.32 (config-if)# shutdown .....	95
7.33 (config-if)# snmp-server.....	95
7.34 (config-if)# spanning-tree.....	95
7.35 (config-if)# speed.....	96
7.36 (config-if)# switchport .....	97
7.37 (config-if)# udld .....	98
<b>8. VLAN Interface Configuration Commands .....</b>	<b>100</b>
8.1 VLAN Interface Configuration.....	100
8.2 (config-if-vlan)# do.....	100
8.3 (config-if-vlan)# end.....	101
8.4 (config-if-vlan)# exit .....	101
8.5 (config-if-vlan)# help .....	101
8.6 (config-if-vlan)# ip.....	101
8.7 (config-if-vlan)# ipv6 .....	103
8.8 (config-if-vlan)# no.....	104



# 1. Introduction

---

## 1.1 Command Modes

You use ICLI (Industrial Command Line Interface) to access the software embedded in your Gigabit Ethernet switches. Because the ICLI is divided into many different modes, the commands available to you at any given time depend on the mode you are currently in. Entering a question mark (?) at the ICLI prompt allows you to obtain a list of commands available for each command mode.

The table below illustrates how to access and exit various command modes of the software.

Command Mode	Access Method	Prompt	Exit Method
EXEC (Limited commands)	<u>Login</u> Username: Password:	#	logout command
Privileged EXEC (All commands)	enable command	#	disable command
Global Configuration	configure terminal command	(config)#	exit command end command <b>Ctrl-Z</b>
Port Interface Configuration	interface command	(config-if)#	exit command to return to Global Configuration mode end command or <b>Ctrl-Z</b> to return to Privileged EXEC mode
VLAN Interface Configuration	interface command	(config-if-vlan)#	exit command to return to Global Configuration mode end command or <b>Ctrl-Z</b> to return to Privileged EXEC mode

## 1.2 Getting Help

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands:

Command	Purpose
help	A brief of command information under the command mode
<i>Abbreviated-command-entry?</i>	Provides a list of commands that begin with a particular character string. (No space between command and "?".)
<i>Abbreviated-command-entry&lt;Tab&gt;</i>	Completes a partial command name

?	List all commands available for the current command mode.
<i>command</i> ?	Lists the keywords or parameters that you must enter next on the command line. (Space between command and question mark.)

### 1.3 Finding Command Options

The following table shows examples how to find command options:

Command	Description
# configure terminal (config)#	Enter the command to enter global configuration mode. You are in global configuration mode when the prompt changes to (config)#.
(config)# <Tab>	List the available command names in global configuration mode.
(config)# ?	List the available commands and brief description in global configuration mode.
(config)# interface ? * All switches or All ports GigabitEthernet 1 Gigabit Ethernet Port vlan VLAN interface configurations	Enter the command to select target interfaces. The available interfaces are: *, GigabitEthernet, and vlan.
(config)# interface * (config-if)#	Enter the command to enter interface configuration mode for all switched ports. You are in port interface configuration mode when the prompt changes to (config-if)#.
(config)# interface GigabitEthernet ? <port_type_list> Port list in 1/1-24 (config)# interface GigabitEthernet 1/1-8 (config-if)#	Enter the command to enter port interface configuration mode for the selected switched port range. 1/ : The switch number (the only one) n-m : Port range from Port #n to Port #m You are in port interface configuration mode when the prompt changes to (config-if)#.
(config-if)# <Tab> access-list aggregation do ... duplex end ...	List the available command names in port interface configuration mode.

...	
<pre>(config-if)# ? access-list  Access list aggregation  Create an aggregation do           To run exec commands in config mode ...</pre>	List the available commands and brief description in port interface configuration mode.
<pre>(config)# interface vlan ? &lt;vlan_list&gt; List of VLAN interface numbers, 1~4095 (config)# interface vlan 2 (config-if-vlan)#</pre>	<p>Enter the command to enter vlan interface configuration mode for the selected vlan range.</p> <p>n : VLAN n n-m : VLAN n to VLAN m</p> <p>You are in vlan interface configuration mode when the prompt changes to <code>(config-if-vlan)#</code>.</p>
<pre>(config-if-vlan)# &lt;Tab&gt; do  end  exit  help  ip  ipv6  no</pre>	List the available command names in vlan interface configuration mode.
<pre>(config-if-vlan)# ? Do      To run exec commands in config mode End     Go back to EXEC mode Exit    Exit from current mode Help    Description of the interactive help system ...</pre>	List the available commands and brief description in vlan interface configuration mode.

## 1.4 Ethernet Interface Naming

An Ethernet interface (“port”) is identified by three pieces of information:

- Its type: FastEthernet, GigabitEthernet, 2.5GigabitEthernet, 5GigabitEthernet, 10GigabitEthernet
- The switch it belongs to. For non-stacking systems this value is always 1. The switch referred in this guide is non-stacking system.
- The port number within the type and switch; the numbering starts with 1 for each type, so a switch may have e.g. both GigabitEthernet 1/1 and 2.5GigabitEthernet 1/1

Many ICLI commands accept a list of interfaces. In its simplest form such a list is a sequence of (type, switch ID, port) information separated by whitespace, e.g.: ‘GigabitEthernet 1/3 10GigabitEthernet 1/5’.

The switch ID and the port numbers can be listed either as single numbers, as lists or as sequences. A list is a comma-separated set of single port numbers or sequences, whereas a sequence is of the form: *from-to*.

Examples:

Syntax	Description
GigabitEthernet 1/5	Single gigabit port number 5 on switch 1
GigabitEthernet 1/2,4,10-12	Gigabit ports 2, 4, 10, 11, 12 on switch 1
*	All ports of all types on all switches
<i>type</i> *	All pots of the specified <i>type</i> on all switches

## 2. Terminal Editing

---

### 2.1 Using the Keyboard

The ICLI provides a rich set of eys to assist the user while working with the command line. The functionality is divided into:

- Basic line editing
- Command history
- Context-sensitive help
- Pagination

### 2.2 Basic Line Editing Keys

Basic line editing allows the input of characters to form a command line, while also allowing cursor movement and insertion/deletion of characters and words. The available editing functions and keys are:

Key	Operation
Left / Right	Move one character left/right
Home / Ctrl-A	Move to start of line
End / Ctrl-E	Move to end of line
Del / Ctrl-D	Delete character at cursor
Backspace / Ctrl-H	Delete character to the left of cursor
Ctrl-N	Delete the entire current line
Ctrl-U / Ctrl-X	Delete all characters to the left of the cursor
Ctrl-K	Delete all characters under the cursor and right
Ctrl-W	Delete from cursor to start of word on the left
TAB	Complete word at end-of-line

### 2.3 Command History Keys

A session maintains a non-persistent command history of previously entered command lines. The history can

be up to 32 lines long; once full, a new line will push the oldest entry out.

Key	Operation
Up / Ctrl-P	Previous line in command history
Down	Next line in command history

## 2.4 Context-sensitive Help Keys

The ICLI implements several hundred commands ranging from the very simple to the very complex. It is therefore imperative that the user can be assisted in entering syntactically correct commands as well as discovering relevant commands. These objectives are supported by the context sensitive help features.

Key	Operation
?	Show next possible input and description
? ? / Ctrl-Q	Show syntax of possible command(s)
TAB	Show next possible input without description or expand current word fully if it is unambiguous

The context-sensitive help only displays commands that are accessible at the current session privilege level.

## 2.5 Pagination Control Keys

Pagination appears each time execution of a command causes output of more lines than what has been configured as terminal length. A typical example is the output from 'show running-config'. After the first several lines have been output, the pagination prompt is presented:

Key	Operation
Enter	Display next line of output
Space	Display next page of output
G	Display remainder of output without more pagination
Q / Ctrl-C	Discard remainder of output
Any other key	Display next page of output. Note that certain terminal keys (arrows, Home, End, etc.) may appear as multiple characters to the ICLI, leading to multiple pages being output in quick succession.

## 2.6 Other Special Keys

One additional key is defined as a convenience. It allows the immediate return from any sub-mode to exec mode.

Key	Operation
-----	-----------

Ctrl-Z	Return directly to Exec mode
--------	------------------------------

## 2.7 Terminal Parameters

Each login to the system via the serial console or via telnet or ssh, creates a session. The session is initialized with settings that are configurable from the 'line' configuration sub-mode, but most of them can also be changed from exec mode while the session is active. Such changes are not persistent, however, and are lost when the session is terminated. The table below lists the available settings and the modes where each can be configured.

Setting	Modess	Description
editing	Exec, Line	Enable/disable command line scrolling
exec-banner	Line	Enable/disable display of the Exec banner (configured with 'banner exec ...')
exec-timeout	Exec, Line	Inactivity timer; automatically log out after a period of inactivity. A value of zero disables automatic logout
history	Exec, Line	Length of command history buffer
length	Exec, Line	Terminal length in lines, used for pagination. Zero disables pagination
location	Line	A line of text that describes the terminal location, e.g. "Server room"
motd-banner	Line	Enable/disable display of Message-Of-The-Day banner (configured with 'banner motd ...')
privilege	Line	Assign default privilege level
width	Exec, Line	Terminal width in characters, used for pagination

## 2.8 Using Banner

The system provides three different banners; text that is output as messages to the user:

- The Message Of The Day banner (MOTD), displayed upon connection to the system, or when a console login attempt has timed out
- The Login banner, displayed before the first "Username:" login prompt
- The Exec banner, displayed upon successful login

All of the above are configured in a similar manner, using the 'banner' command:

```
banner [ motd ] banner
```

```
banner exec banner
```

```
banner login banner
```

The banner text can be either a single line or multiple lines. The first character of the text defines a delimiter character; the actual text of the banner then follows and ends at the first appearance of the delimiter character.

Neither of the delimiters are included in the actual text.

## 3. Working with Configuration Files

---

There are four kinds of configuration files:

- ‘`running-config`’, a virtual file containing the currently running system configuration
- ‘`startup-config`’, containing the boot-time configuration. When configuration is changed it must be copied to ‘`startup-config`’ in order to be applied at the next boot
- ‘`default-config`’, read-only and used when configuration is restored to defaults, i.e. also if ‘`startup-config`’ is missing. It contains product-specific customizations to the default settings of the device
- User-defined configuration files, of which there can exist up to two. These are typically used for backups or variants of ‘`startup-config`’

All of these except ‘`running-config`’ are stored in the flash: file system. The available operations are:

*copy source destination*

The source and destination can be one of:

- `running-config`
- `startup-config` (or `flash:startup-config`)
- `flash:filename`
- `tftp://server[:port]/path-to-file`

### 3.1 Reverting to Default Configuration

It is possible to reset the total system configuration to defaults in two ways:

- Deleting ‘`startup-config`’ and rebooting
- Instructing the software to discard current configuration and reset to defaults without rebooting

Deleting ‘`startup-config`’ doesn’t change ‘`running-config`’ until the system is rebooted, at which time defaults are loaded.

Conversely, discarding the current configuration does indeed affect ‘`running-config`’ but does not touch ‘`startup-config`’. An explicit ‘`copy running-config startup-config`’ is necessary to make the change persistent. Rebooting and resetting configuration to defaults is accomplished with the ‘`reload`’ command:

```
reload cold
reload defaults [keep-ip]
```

The first form reboots the system. If the system is stacking, a specific switch can be rebooted as well by supplying its switch ID.

The second form loads configuration defaults. If the ‘`keep-ip`’ keyword is given then the system attempts to keep the most relevant parts of the VLAN 1 IP setup in order to maintain management connectivity: The IP address setup and the active default route.

**Note:** There is no guarantee, however, that the above is sufficient. It depends on the actual network properties and the system’s total IP configuration. In some cases it may be preferable to explicitly un-configure the system using ‘`no`’ commands, or prepare a suitable configuration and download it to the system’s ‘`startup-config`’ and reboot.

## 4. Working with Software Images

---

The system can store up to two software images that are stored in FLASH. The image selected for bootup is termed the Active image, while the other is termed the Alternate image. It is possible to swap the Active and Alternative image, and it is possible to upgrade to a new Active image. A swap simply switches the Active/Alternate designation on each image and reboots the system. A firmware upgrade performs these steps:

- Download new firmware using TFTP and verify suitability for the system
- Overwrite the current Alternate image with the newly downloaded image
- Swap Active/Alternate and reboot

The result is that the old Active build becomes Alternate, and the newly downloaded image Active. The relevant commands are:

```
show version
firmware swap
firmware upgrade tftp://server[:port/path_to_file]
```

‘`show version`’ lists various details about the system, including the images in FLASH.

## 5. Commands in EXEC Mode

---



# ?	
Clear	Reset functions
cls	clear screen
Configure	Enter configuration mode
Copy	Copy from source to destination
Debug	Debugging functions
Delete	Delete one file in flash: file system
Dir	Directory of all files in flash: file system
Disable	Turn off privileged commands
Do	To run exec commands in config mode
dot1x	IEEE Standard for port-based Network Access Control
enable	Turn on privileged commands
exit	Exit from EXEC mode
firmware	Firmware upgrade/swap
help	Description of the interactive help system
ip	IPv4 commands
ipv6	IPv6 configuration commands
logout	Exit from EXEC mode
more	Display file
no	Negate a command or set its defaults
ping	Send ICMP echo messages
platform	Platform configuration
reload	Reload system.
Send	Send a message to other tty lines
Show	Show running system information
Terminal	set terminal line parameters
Veriphy	Veriphy keyword

## 5.1 clear Command

### Options

# clear ?	
access	Access management
access-list	Access list
dot1x	IEEE Standard for port-based Network Access Control
ip	Interface Internet Protocol config commands
ipv6	IPv6 configuration commands

lACP	Clear LACP statistics
lldp	Clears LLDP statistics.
logging	Syslog
mac	MAC Address Table
mvr	Multicast VLAN Registration configuration
sflow	Statistics flow.
spanning-tree	STP Bridge
statistics	Clear statistics for one or more given interfaces

### Syntax

```

clear access management statistics
clear access-list ace statistics
clear dot1x statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]
clear ip arp
clear ip dhcp detailed statistics { server | client | snooping | relay | helper
    | all } [ interface ( <port_type> [ <in_port_list> ] ) ]
clear ip dhcp relay statistics
clear ip dhcp server binding <ip>
clear ip dhcp server binding type { automatic | manual | expired }
clear ip dhcp server statistics
clear ip dhcp snooping statistics [ interface ( <port_type> [ <in_port_list> ] ) ]
clear ip igmp snooping [ vlan <v_vlan_list> ] statistics
clear ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ]
    [ icmp-msg <type> ]
clear ipv6 mld snooping [ vlan <v_vlan_list> ] statistics
clear ipv6 neighbors
clear ipv6 statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ]
    [ icmp-msg <type> ]
clear lacp statistics
clear lldp statistics { [ interface ( <port_type> [ <p_list> ] ) ] | global }
clear logging [ informational ] [ notice ] [ warning ] [ error ] [ switch <switch_
h_list> ]
clear mac address-table
clear mvr [ vlan <v_vlan_list> | name <mvr_name> ] statistics
clear sflow statistics { receiver [ <receiver_index_list> ] | samplers
    [ interface [ <samplers_list> ] ( <port_type> [ <v_port_type_list> ] ) ] }
clear spanning-tree { { statistics [ interface ( <port_type>

```

```
[ <v_port_type_list> ] ) ] } | { detected-protocols [ interface ( <port_type>
[ <v_port_type_list_1> ] ) ] } }
clear statistics [ interface ] ( <port_type> [ <v_port_type_list> ] )
```

## 5.2 cls command

### Options

```
# cls ?
    <1-100000>  Set number of new lines
    <cr>        Clear screen
```

### Syntax

```
# cls ?
cls [ <n> ]
```

## 5.3 configure Command

To enter global configuration mode or to configure the system from the RAM memory, use the `configure terminal` privileged EXEC command.

Use this command to enter global configuration mode. Note that commands in this mode are written to the running configuration file as soon as you enter them (using the Enter key or Carriage Return).

After you enter the configure command, the system prompt changes from `#` to `(config)#`, indicating that the switch is in global configuration mode.

```
# Configure terminal
(config)#
```

## 5.4 copy Command

To copy any file from a source to a destination, use the copy EXEC command.

### Syntax

```
# copy ?
copy { startup-config | running-config | <source_path> } { startup-config | running-config | <destination_path> } [ syntax-check ]
```

### Keywords

running-config      Currently running configuration file in system  
startup-config      Startup configuration file in flash used during system boot-up

### Parameters

<source\_path>      flash:filename (file in system flash) |  
                      tftp://server/path-and-filename (file on TFTP server)  
<destination\_path> flash:filename | tftp://server/path-and-filename  
                      A valid file name is a text string drawn from alphabet (A-Za-z),  
                      digits (0-9), dot (.), hyphen (-), under score(\_). The maximum  
                      length is 63 and hyphen must not be first character. The file name  
                      content that only contains '.' is not allowed.

## 5.5 debug Command

### Options

# debug ?  
    ip            Interface Internet Protocol config commands  
    prompt      Set prompt for testing

### Syntax

# debug ?  
debug ip dhcp helper frame information  
debug prompt <debug\_prompt>

## 5.6 delete Command

To delete a file from the system flash memory, use the delete EXEC command.

### Option

# delete ?  
    <Path>      Name of file or directory to delete

### Syntax

delete <path>

## 5.7 dir Command

### Option

# dir ?

|           Output modifiers  
<cr>       display current directory in flash

Syntax

# dir ?

dir

## 5.8 do Command

Options

# do line ?

line   Exec Command

<cr>

Syntax

do <command>

# do

## 5.9 dot1x Command

To perform authentication for the specified interfaces, enter dot1x EXEC command, IEEE Standard for port-based Network Access Control command.

Description

# dot1x ?

initialize   Force re-authentication immediately

Syntax

dot1x initialize [ interface ( <port\_type> [ <plist> ] ) ]

Parameters

<port_type>	*	All switches or All ports
	FastEthernet	Fast Ethernet Port
	GigabitEthernet	1 Gigabit Ethernet Port
	10GigabitEthernet	10 Gigabit Ethernet Port
<plist>	Port list	

## 5.10 enable Command

Turn on privileged commands

### Options

```
# enable ?  
    <0-15>    Choose privileged level  
    <cr>
```

### Syntax

```
# enable ?  
enable [ <new_priv> ]
```

## 5.11 exit Command

Use the exit command in EXEC mode to exit the active CLI connection (log off the switch). Or use the exit command to exit different configuration modes.

### Description

```
# exit ?  
    <cr>    Exit from current mode
```

### Syntax

Exit

#### Example: Exit privilege EXEC mode to logoff the switch

```
# exit
```

#### Example: Exit user EXEC mode to logoff the switch

```
> exit
```

#### Example: Exit global configuration mode to privilege EXEC mode

```
(config)# exit  
#
```

#### Example: Exit interface configuration mode to global configuration mode

```
(config-if)# exit  
(config)#
```

## 5.12 firmware Command

Two firmware images are embedded in the system. The active image is the one used during system boot-up. The alternative one is the previous active image after it was upgraded by the current active image.

### Options

# firmware ?

swap        Swap between Active and Alternate firmware image.  
upgrade     Firmware upgrade

### Syntax

firmware swap

firmware upgrade <url\_file>

### Parameter

<url\_file>: firmware file located in tftp server

## 5.13 help Command

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?').

## 5.14 ip Command

To enable DHCP client for the specified VLAN interface, use the ip EXEC command.

### Option

# ip ?

dhcp        Dhcp commands

### Syntax

ip dhcp retry interface vlan <vlan\_id>

### Parameter

<vlan\_id>    vlan ID

## 5.15 ipv6 Command

### Option

```
# ipv6 ?  
    dhcp-client    Manage DHCPV6 client service
```

### Syntax

```
ipv6 dhcp-client restart [ interface vlan <v_vlan_list> ]
```

### Parameter

```
<vlan_list>    IPv6 interface VLAN list
```

## 5.16 logout Command

To exit the active CLI session in EXEC mode, use the logout EXEC command.

### Syntax

```
logout
```

### Example:

```
# logout
```

### Example:

```
> logout
```

## 5.17 more Command

To display a file, use the more EXEC command.

### Option

```
# more ?  
    <path>    File in FLASH or on TFTP server
```

### Syntax

```
more <path>
```

### Parameter

```
<path>    flash:filename or tftp://server[:port]/path-to-file  
A valid file name is a text string drawn from alphabet (A-Za-z), digits  
(0-9), dot (.), hyphen (-), under score(_). The maximum length is 63 and
```



hyphen must not be first character. The file name content that only contains '.' is not allowed.

## 5.18 no Command

To disable specific functions or return to default values, use the no EXEC command.

### Options

# no ?

debug	Debugging functions
port-security	Port security (psec limit)
terminal	Set terminal line parameters

# no terminal ?

editing	No command line editing feature
exec-timeout	No the EXEC timeout
history	No the command history function
length	Default number of lines on a screen
width	Default width of the display terminal

### Syntax

```
no debug interrupt-monitor source <source>
no debug ipv6 nd
no debug trace hunt
no port-security shutdown [ interface ( <port_type> [ <v_port_type_list> ] ) ]
no terminal editing
no terminal exec-timeout
no terminal history size
no terminal length
no terminal width
```

### Parameters

Nd	IPv6 Neighbor Discovery debugging
<source>	The possible values are enum vtss_interrupt_source_t values found in file board/interrupt_api.h

## 5.19 ping Command

To ping an ICMP device, use the ping EXEC command.

### Options

# ping ?

ip IP (ICMP) echo  
ipv6 IPV6 (ICMPV6) echo

### Syntax

```
ping ip <v_ip_addr> [ repeat <count> ] [ size <size> ] [ interval <seconds> ]  
ping ipv6 <v_ipv6_addr> [ repeat <count> ] [ size <size> ] [ interval <seconds>  
] [ interface vlan <v_vlan_id> ]
```

### Parameters

<v\_ip\_addr> Target IP address  
<count> The number of ping packets that will be sent to the destination address.  
The default is 5 packets.  
<size> The size of the ping packet (in bytes). The default is 100 bytes.  
<seconds> The timeout interval. The default is 2 seconds.

## 5.20 platform Command

Platform configuration

### Options

# platform ?

debug Debug command setting

### Syntax

```
platform debug { allow | deny }
```

### Parameters

Allow Allow debug commands  
Deny Deny debug commands

## 5.21 reload Command

To reboot the system or reload the default configuration without rebooting, use the reload EXEC command.

### Options

# reload ?

cold Reload cold.

defaults      Reload defaults without rebooting.

#### Syntax

```
reload { cold | { defaults [ keep-ip ] }
```

#### Parameters

keep-ip      Attempt to keep VLAN1 IP setup.

## 5.22 send Command

To send messages to one or all terminal lines, use the send EXEC command.

#### Options

# send ?

*	All tty lines
<session_list>	Send a message to multiple lines
console	Primary terminal line
vty	Virtual terminal

#### Syntax

```
send { * | <session_list> | console 0 | vty <vty_list> } <message>
```

#### Parameters

<session_list>	0~16
<vty_list>	0~15
<message>	<line128> Message to be sent to lines, in 128 char's

## 5.23 show Command

To show current system configuration and status, use the show EXEC command.

#### Options

# show ?

Aaa	Authentication, Authorization and Accounting methods
Access	Access management
access-list	Access list
aggregation	Aggregation port configuration
clock	Configure time-of-day clock
dot1x	IEEE Standard for port-based Network Access Control

green-ethernet	Green ethernet (Power reduction)
history	Display the session command history
interface	Interface status and configuration
ip	Internet Protocol
ipmc	IPv4/IPv6 multicast configuration
ipv6	IPv6 configuration commands
lacp	LACP configuration/status
line	TTY line information
lldp	Display LLDP neighbors information.
Logging	System logging message
loop-protect	Loop protection configuration
mac	Mac Address Table information
mvr	Multicast VLAN Registration configuration
ntp	Configure NTP
platform	Platform configuration
port-security	Port Security status - Port Security is a module with no direct configuration.
Privilege	Display command privilege
Process	process
Pvlan	PVLAN configuration
Qos	Quality of Service
radius-server	RADIUS configuration
rmon	RMON statistics
running-config	Show running system information
sflow	Statistics flow.
sfpddm	Display SFP DDM status for the switch.
snmp	Display SNMP configurations
spanning-tree	STP Bridge
switchport	Display switching mode characteristics
system	system
tacacs-server	TACACS+ configuration
terminal	Display terminal configuration parameters
udld	Uni Directional Link Detection(UDLD) configurations, statistics and status
upnp	Display UPnP configurations
user-privilege	Users privilege configuration
users	Display information about terminal lines

version	System hardware and software status
vlan	VLAN status
voice	Voice appliance attributes
web	web

### Syntax

```

show aaa
show access management [ statistics | <access_id_list> ]
show access-list [ interface ( ( <port_type> [ <v_port_type_list> ] ) ) ] [ rate
-limiter [ <rate_limiter_list> ] ] [ ace statistics [ <ace_list> ] ]
show access-list ace-status [ static ] [ link-oam ] [ loop-protect ] [ dhcp ] [
ptp ] [ upnp ] [ arp-inspection ] [ evc ] [ mep ] [ ipmc ] [ ip-source-guard ] [
ip-mgmt ] [ tt-loop ] [ y1564 ] [ ztp ] [ conflicts ] [ switch <switch_list> ]
show aggregation [ mode ]
show clock
show clock detail
show dot1x statistics { eapol | radius | all } [ interface ( <port_type> [ <v_po
rt_type_list> ] ) ]
show dot1x status [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ brief ]
show green-ethernet [ interface ( <port_type> [ <port_list> ] ) ]
show green-ethernet eee [ interface ( <port_type> [ <port_list> ] ) ]
show green-ethernet energy-detect [ interface ( <port_type> [ <port_list> ] ) ]
show green-ethernet short-reach [ interface ( <port_type> [ <port_list> ] ) ]
show history
show interface ( <port_type> [ <in_port_list> ] ) switchport [ access | trunk |
hybrid ]
show interface ( <port_type> [ <v_port_type_list> ] ) capabilities
show interface ( <port_type> [ <v_port_type_list> ]
ytes | errors | discards | filtered | { priority [ <priority_v_0_to_7> ] } } ] [
{ up | down } ]
show interface ( <port_type> [ <v_port_type_list> ] ) status
show interface ( <port_type> [ <v_port_type_list> ] ) veriphy
show interface vlan [ <vlist> ]
show ip arp
show ip arp inspection [ interface ( <port_type> [ <in_port_type_list> ] ) | vla
n <in_vlan_list> ]
show ip arp inspection entry [ dhcp-snooping | static ] [ interface ( <port_type

```

```

> [ <in_port_type_list> ] ) ]
show ip dhcp detailed statistics { server
orward | combined } [ interface ( <port_type> [ <in_port_list> ] ) ]
show ip dhcp excluded-address
show ip dhcp pool [ <pool_name> ]
show ip dhcp relay [ statistics ]
show ip dhcp server
show ip dhcp server binding <ip>
show ip dhcp server binding [ state { allocated | committed | expired } ] [ type
{ automatic | manual | expired } ]
show ip dhcp server declined-ip
show ip dhcp server declined-ip <declined_ip>
show ip dhcp server statistics
show ip dhcp snooping [ interface ( <port_type> [ <in_port_list> ] ) ]
show ip dhcp snooping table
show ip domain
show ip http server secure status
show ip igmp snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <por
t_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
show ip igmp snooping mrouter [ detail ]
show ip interface brief
show ip name-server
show ip route
show ip source binding [ dhcp-snooping | static ] [ interface ( <port_type> [ <i
n_port_type_list> ] ) ]
show ip ssh
show ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ ic
sg <type> ]
show ip verify source [ interface ( <port_type> [ <in_port_type_list> ] ) ]
show ipmc profile [ <profile_name> ] [ detail ]
show ipmc range [ <entry_name> ]
show ipv6 dhcp-client [ interface vlan <v_vlan_list> ]
show ipv6 interface [ vlan <v_vlan_list> { brief | statistics } ]
show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <po
rt_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
show ipv6 mld snooping mrouter [ detail ]
show ipv6 neighbor [ interface vlan

```

```

show ipv6 route [ interface vlan <v_vlan_list> ]
show ipv6 statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp
-msg <type> ]
show lacp { internal | statistics | system-id | neighbor }
show line [ alive ]
show lldp eee [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show lldp med media-vlan-policy [ <v_0_to_31> ]
show lldp med remote-device [ interface ( <port_type> [ <port_list> ] ) ]
show lldp neighbors [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show lldp statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show logging <log_id> [ switch <switch_list> ]
show logging [ informational ] [ notice ] [ warning ] [ error ] [ switch <switch
_list> ]
show loop-protect [ interface ( <port_type> [ <p_list> ] ) ]
show mac address-table [ conf | static | aging-time | { { learning | count } [ i
nterface ( <port_type> [ <v_port_type_list> ] ) | vlan <v_vlan_id_2> ] } | { add
ress <v_mac_addr> [ vlan <v_vlan_id> ] } | vlan <v_vlan_id_1> | interface ( <por
t_type> [ <v_port_type_list_1> ] ) ]
show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface (
<port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
show ntp status
show platform debug
show platform phy [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show platform phy id [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show platform phy instance
show platform phy mode [ interface ( <port_type> [ <v_por
show poe [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show port-security switch [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show privilege
show process list [ detail ]
show process load
show pvlan [ <pvlan_list> ]
show pvlan isolation [ interface ( <port_type> [ <p_list> ] ) ]
show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-c
os ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ]
ranslation ] } | storm | { qce [ <qce> ] } ]

```

```

show radius-server [ statistics ]
show rmon alarm [ <id_list> ]
show rmon event [ <id_list> ]
show rmon history [ <id_list> ]
show rmon statistics [ <id_list> ]
show running-config [ all-defaults ]
show running-config feature <feature_name> [ all-defaults ]
show running-config interface ( <port_type> [ <list> ] ) [ all-defaults ]
show running-config interface vlan <list> [ all-defaults ]
show running-config line { console | vty } <list> [ all-defaults ]
show running-config vlan { [ <vlan_list> ] } [ all-defaults ]
show sflow
show sflow statistics { receiver [ <rcvr_idx_list> ] | samplers [ interface [ <s
amplers_list> ] ( <port_type> [ <v_port_type_list> ] ) ] }
show sfpddm
show snmp
show snmp access [ <group_name> { v1 | v2c | v3 | any } { auth | noauth | priv }
]
show snmp community v3 [ <community> ]
show snmp host [ <conf_name> ] [ system ] [ switch ] [ interface ] [ aaa ]
show snmp mib context
show snmp mib ifmib ifIndex
show snmp security-to-group [ { v1
show snmp user [ <username> <engineID> ]
show snmp view [ <view_name> <oid_subtree> ]
show spanning-tree [ summary | active | { interface ( <port_type> [ <v_port_typ
_list> ] ) } | { detailed [ interface ( <port_type> [ <v_port_type_list_1> ] ) ]
} | { mst [ configuration | { <instance> [ interface ( <port_type> [ <v_port_ty
pe_list_2> ] ) ] } ] } ] } ]
show switchport forbidden [ { vlan <vlan_list> } | { name <name> } ]
show system cpu status
show system led status
show tacacs-server
show terminal
show udld [ interface ( <port_type> [ <plist> ] ) ]
show upnp
show user-privilege

```



```

show users [ myself ]
show version [ brief ]
show vlan [ id <vlan_list> | name <name> | brief ] [ all ]
show vlan ip-subnet [ <ipv4> ]
show vlan mac [ address <mac_addr> ]
show vlan protocol [ eth2 { <etype> | arp | ip | ipx | at } ] [ snap { <oui> | r
fc-1042 | snap-8021h } <pid> ] [ llc <dsap> <ssap> ]
show vlan status [ interface ( <port_type> [ <plist> ] ) ] [ admin | all | combi
ned | conflicts | erps | evc | gvrp | mep | mstp | mvr | nas | rmirror | vcl | v
oice-vlan ]
show voice vlan [ oui <oui> | interface ( <port_type> [ <port_list> ] ) ]
show web privilege group [ <group_name> ] level

```

## 5.24 terminal Command

### Options

# terminal ?

editing	Enable command line editing
exec-timeout	Set the EXEC timeout in minutes 0 ~ 1440
help	Description of the interactive help system
history	Control the command history function
length	Set number of lines on a screen
width	Set width of the display terminal

### Syntax

```

terminal editing
terminal exec-timeout <min> [ <sec> ]
terminal help
terminal history size <history_size>
terminal length <lines>
terminal width <width>

```

### Parameters

<min>	0-1440
<history_size>	0-32 (0 - disable)
<lines>	Number of lines on screen, 0 or 3-512 (0 for no pausing)
<width>	Number of characters on a screen line, 0 or 40-512

(0 for unlimited width)

## 5.25 veriphy Command

### Options

```
# veriphy ?  
    interface  Interface keyword  
    <cr>
```

### Syntax

```
veriphy [ { interface ( <port_type> [ <v_port_type_list> ] ) } ]
```

### Parameters

<port_type>	* (All switches or All ports) FastEthernet (Fast Ethernet Port) GigabitEthernet (1 Gigabit Ethernet Port) 10GigabitEthernet (10 Gigabit Ethernet Port)
<port_type_list>	Port list for all port types

## 6. Global Configuration Commands

---

To enter global configuration mode, use the configure terminal command.

### Commands

```
# configure terminal
```

```
(config)# ?
```

Aaa	Authentication, Authorization and Accounting
Access	Access management
access-list	Access list
aggregation	Aggregation mode
banner	Define a login banner
clock	Configure time-of-day clock
default	Set a command to its defaults
do	To run exec commands in config mode
dot1x	IEEE Standard for port-based Network Access Control
enable	Modify enable password parameters
end	Go back to EXEC mode
exit	Exit from current mode
green-ethernet	Green ethernet (Power reduction)
gvrp	Enable GVRP feature
help	Description of the interactive help system
hostname	Set system's network name
interface	Select an interface to configure
ip	Internet Protocol
ipmc	IPv4/IPv6 multicast configuration
ipv6	IPv6 configuration commands
json	JavaScript Object Notation RPC
lACP	LACP settings
line	Configure a terminal line
lldp	LLDP configurations.
Logging	System logging message
loop-protect	Loop protection configuration
mac	MAC table entries/configuration
monitor	Mirror configuration
mvr	Multicast VLAN Registration configuration
no	Negate a command or set its defaults

ntp	Configure NTP
poe	Power Over Ethernet.
port-security	Enable/disable port security globally.
Privilege	Command privilege parameters
Qos	Quality of Service
radius-server	Configure RADIUS
rmon	Remote Monitoring
sflow	Statistics flow.
snmp-server	Set SNMP server's configurations
spanning-tree	Spanning Tree protocol
tacacs-server	Configure TACACS+
udld	Enable UDLD in the aggressive or normal mode and to set the configurable message timer on all fiber-optic ports.
Upnp	Set UPnP's configurations
Username	Establish User Name Authentication
vlan	VLAN commands
voice	Voice appliance attributes
web	Web

## 6.1 aaa command

### Description

(config)# aaa ?

Accounting	Accounting
Authentication	Authentication
Authorization	Authorization

### Syntax

```
aaa accounting { console | telnet | ssh } tacacs { [ commands <priv_lvl> ] [ exe
c ] }*1
```

```
aaa authentication login { console | telnet | ssh | http } { { local | radius |
tacacs } [ { local | radius | tacacs } [ { local | radius | tacacs } ] ] }
```

```
aaa authorization { console | telnet | ssh } tacacs commands <priv_lvl> [ config
-commands ]
```

### keywords

console	Configure Console command accounting
---------	--------------------------------------

ssh	Configure SSH command accounting
telnet	Configure Telnet command accounting
tacacs	Use TACACS+ for accounting
commands	Enable command accounting
exec	Enable EXEC accounting
http	Configure HTTP authentication
local	Use local database for authentication
radius	Use RADIUS for authentication
tacacs	Use TACACS+ for authentication

#### Parameters

<priv\_lvl>  
 <0-15> Command privilege level. Commands >= this level are accounted

## 6.2 access command

#### Description

(config)# access ?

management Access management configuration

#### Syntax

access management

access management <access\_id> <access\_vid> <start\_addr> [ to <end\_addr> ]  
 { [ web ] [ snmp ] [ telnet ] | all } (null)

#### Parameters

<AccessId : 1-16>: ID of access management entry

<AccessVid : 1-4095>: The VLAN ID for the access management entry

<AddrRangeStart : ipv4\_addr>: Start IPv4 address

<AddrRangeStart : ipv6\_addr>: Start IPv6 address

<AddrRangeEnd : ipv4\_addr>: End IPv4 address

<AddrRangeEnd : ipv6\_addr>: End IPv6 address

#### Keywords

all All services

snmp SNMP service

telnet TELNET/SSH service

to End address of the range  
web web service

## 6.3 access-list Command

### Option

```
(config)# access-list ?  
  ace          Access list entry  
  rate-limiter Rate limiter
```

### Keywords

Action	Access list action
dmac-type	The type of destination MAC address
frame-type	Frame type
ingress	Ingress
logging	Logging frame information. Note: The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.
Mirror	Mirror frame to destination mirror port
Next	insert the current ACE before the next ACE ID
Policy	Policy
rate-limiter	Rate limiter
redirect	Redirect frame to specific port
shutdown	Shutdown incoming port. The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).
Tag	Tag
tag-priority	Tag priority
vid	VID field
<1-512>	ACE ID
Update	Update an existing ACE
10pps	10 packets per second
25kbps	25k bits per second
<1~16>	Rate limiter ID

### Parameters

<0-400000>      Rate value  
<0-500000>      Rate value

## 6.4 aggregation Command

### Options

```
(config)# agg ?  
aggregation mode { [ smac ] [ dmac ] [ ip ] [ port ] }*1
```

### Keywords

dmac    Destination MAC affects the distribution  
ip      IP address affects the distribution  
port    IP port affects the distribution  
smac    Source MAC affects the distribution

## 6.5 banner Command

### Options

```
(config)# banner ?  
  <line>      c banner-text c, where 'c' is a delimiting character  
  Exec        Set EXEC process creation banner  
  Login       Set login banner  
  Motd        Set Message of the Day banner
```

### Syntax

```
banner [ exec | login | motd ] [ <banner> ]
```

### Parameters

<banner>    c banner-text c, where 'c' is a delimiting character

### Example to set banner “Good Day” when entering EXEC mode

```
(config)# banner exec c Goog Day c
```

## 6.6 clock Command

### Options

```
(config)# clock ?
```

summer-time      Configure summer (daylight savings) time  
timezone          Configure time zone

#### Syntax

```
clock summer-time <word16> date [ <start_month_var> <start_date_var>
    <start_year_var> <start_hour_var> <end_month_var> <end_date_var> <end_year_var>
    <end_hour_var> [ <offset_var> ] ]
clock summer-time <word16> recurring [ <start_week_var> <start_day_var>
    <start_month_var> <start_hour_var> <end_week_var> <end_day_var> <end_month_var>
    <end_hour_var> [ <offset_var> ] ]
clock timezone <word_var> <hour_var> [ <minute_var> ]
```

## 6.7 default Command

#### Option

```
(config)# default ?
    access-list    Access list
```

#### Syntax

```
default access-list rate-limiter [ <rate_limiter_list> ]
```

#### Parameter

```
<RateLimiterId : 1-16>    Rate limiter ID
```

## 6.8 do Command

To perform EXEC command in global configuration mode, use the do command.

#### Option

```
(config)# do ?
    LINE    Exec Command
```

#### Syntax

```
do <command>
```

## 6.9 dot1x Command

#### Options



(config)# dot1x ?

authentication	Authentication
feature	Globally enables/disables a dot1x feature functionality
guest-vlan	Guest VLAN
max-reauth-req	The number of times a Request Identity EAPOL frame is sent without response before considering entering the Guest VLAN
re-authentication	Set Re-authentication state
system-auth-control	Set the global NAS state
timeout	timeout

### Syntax

```
dot1x authentication timer inactivity <v_10_to_100000>
dot1x authentication timer re-authenticate <v_1_to_3600>
dot1x feature { [ guest-vlan ] [ radius-qos ] [ radius-vlan ] }*1
dot1x guest-vlan <value>
dot1x guest-vlan supplicant
dot1x max-reauth-req <value>
dot1x re-authentication
dot1x system-auth-control
dot1x timeout quiet-period <v_10_to_1000000>
dot1x timeout tx-period <v_1_to_65535>
```

### Keywords & Parameters

timer	timer
inactivity	Time in seconds between check for activity on successfully authenticated MAC addresses.
re-authenticate	The period between re-authentication attempts in seconds
guest-vlan	Globally enables/disables state of guest-vlan
radius-qos	Globally enables/disables state of RADIUS-assigned QoS.
radius-vlan	Globally enables/disables state of RADIUS-assigned VLAN.
<1-4095>	Guest VLAN ID used when entering the Guest VLAN.
supplicant	The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled.

## 6.10 enable Command

### Options

(config)# enable ?

password	Assign the privileged level clear password
secret	Assign the privileged level secret

### Syntax

enable password [ level <priv> ] <password>

enable secret { 0 | 5 } [ level <priv> ] <password>

### Parameters

<password>	The UNENCRYPTED (cleartext) password
level	Set exec level password
<priv>	0 - 15
0	Specifies an UNENCRYPTED password will follow
5	Specifies an ENCRYPTED secret will follow

## 6.11 end Command

To exit global configuration mode to EXEC mode, use the end command.

### Syntax

end

### Example:

```
(config)# end
#
```

## 6.12 exit Command

To exit global configuration mode to EXEC mode, use the exit command.

### Syntax

exit

### Example:

```
(config)# exit
#
```

## 6.13 gvrp Command

### Options

```
(config)# gvrp ?
  max-vlans    Number of simultaneous VLANs that GVRP can control
  time         Configure GARP protocol timer parameters. IEEE 802.1D-2004,
              clause 12.11.
```

### Syntax

```
gvrp max-vlans <maxvlans>
gvrp time { [ join-time <jointime> ] [ leave-time <leavetime> ]
           [ leave-all-time <leavealltime> ] }*1
```

### Parameters

```
<maxvlans>    1-4095
join-time     Set GARP protocol parameter JoinTime. See IEEE
              802.1D-2004, clause 12.11
leave-all-time Set GARP protocol parameter LeaveAllTime. See IEEE
              802.1D-2004, clause 12.11
leave-time    Set GARP protocol parameter LeaveTime. See IEEE
              802.1D-2004, clause 12.11
```

## 6.14 help Command

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?'.)

## 6.15 hostname Command

To specify or modify the host name for the switch, use the hostname global configuration command. The factory-assigned default host name is null.

### Option

```
(config)# hostname ?  
    WORD    This system's network name
```

### Syntax

```
hostname <hostname>
```

## 6.16 interface Command

To enter interface configuration mode, use the interface command. The target interfaces include the switched ports and VLANs. For Gigabit Ethernet port interface the prompt is changed to **(config-if)#**. For VLAN interface the prompt is changed to **(config-if-vlan)#**. The available commands for the interface configuration mode are described in Chapter 4.

### Options

```
(config)# interface ?  
    *                All switched ports  
    FastEthernet    Fast Ethernet Port  
    GigabitEthernet 1 switched Port  
    10GigabitEthernet 10 Gigabit Ethernet Port  
    vlan            VLAN interface configurations
```

### Syntax

```
interface ( <port_type> [ <plist> ] )  
interface vlan <vlist>
```

### Example

```
(config)# interface GigabitEthernet 1  
(config-if)#
```

### Example

```
(config)# interface vlan 1  
(config-if-vlan)#
```

## 6.17 ip Commands

The optional commands are:

```
(config)# ip ?
  arp          Address Resolution Protocol
  dhcp         Dynamic Host Configuration Protocol
  domain       IP DNS Resolver
  dns          Domain Name System
  helper-address DHCP relay server
  http         Hypertext Transfer Protocol
  igmp         Internet Group Management Protocol
  name-server  Domain Name System
  route        Add IP route
  routing      Enable routing for IPv4 and IPv6
  source       Source command
  ssh          Secure Shell
  verify       Verify command
```

## 6.18 ip arp Command

### Syntax

```
(config)# ip arp ?
ip arp inspection
ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var>
    <ipv4_var>
ip arp inspection translate [ interface <port_type> <in_port_type_id> <vlan_var>
    <mac_var> <ipv4_var> ]
ip arp inspection vlan <in_vlan_list>
ip arp inspection vlan <in_vlan_list> logging { deny | permit | all }
```

### Parameters

```
<port_type>      GigabitEthernet (1 Gigabit Ethernet Port)
<port_type_id>  Port ID in 1/1-24
<vlan_id>       Select a VLAN id to configure
<mac_var>       Select a MAC address to configure
<ipv4_var>      Select an IP Address to configure
<in_vlan_list>  arp inspection vlan list
all              log all entries
deny            log denied entries
permit          log permitted entries
```

## 6.19 ip dhcp Command

### Syntax

```
ip dhcp excluded-address <low_ip> [ <high_ip> ]
ip dhcp pool <pool_name>
ip dhcp relay
ip dhcp relay information option
ip dhcp relay information policy { drop | keep | replace }
ip dhcp server
ip dhcp snooping
```

### Keywords

excluded-address	Prevent DHCP from assigning certain addresses
pool	Configure DHCP address pools
relay	DHCP relay agent configuration
server	Enable DHCP server
snooping	DHCP snooping
information	DHCP information option (Option 82)
option	DHCP option
policy	Policy for handling the receiving DHCP packet already include the information option
drop	Drop the package when receive a DHCP message that already contains relay information
keep	Keep the original relay information when receive a DHCP message that already contains it
replace	Replace the original relay information when receive a DHCP message that already contains it

### Parameters

<low_ip>	A.B.C.D format, Low IP address
<high_ip>	A.B.C.D format, High IP address
<pool_name>	Pool name in 32 characters

## 6.20 ip dns Command

### Option

```
(config)# ip dns ?  
    proxy    DNS proxy service
```

#### Syntax

```
ip dns proxy
```

## 6.21 ip domans Command

#### Syntax

```
(config)# ip domain name ?  
ip domain name { <v_domain_name> | dhcp [ ipv4 | ipv6 ] [ interface vlan <v_vlan  
_id_dhcp> ] }
```

#### Keywords

```
dhcp            Dynamic Host Configuration Protocol  
ipv4  
ipv6  
interface  
vlan
```

#### Parameters

```
<domain_name>  Default domain name  
<v_vlan_id>    VLAN ID
```

## 6.22 ip helper-address Command

```
(config)# ip helper-address ?  
    <Ip : ipv4_ucast>    IP address of the DHCP relay server
```

#### Syntax

```
ip helper-address <v_ipv4_ucast>
```

## 6.23 ip http Command

#### Options

```
ip http secure-certificate { upload <url_file> [ pass-phrase <pass_phrase> ] | d  
elete | generate }
```

```
ip http secure-redirect
ip http secure-server
```

### Keywords

secure-certificate	HTTPS certificate
secure-redirect	Secure HTTP web redirection
secure-server	Secure HTTP web server
delete	Delete the current certificate
generate	Generate a new self-signed RSA certificate
upload	Upload a certificate PEM file

## 6.24 ip igmp Command

### Syntax

```
ip igmp host-proxy [ leave-proxy ]
ip igmp snooping
ip igmp snooping vlan <v_vlan_list>
ip igmp ssm-range <v_ipv4_mcast> <ipv4_prefix_length>
ip igmp unknown-flooding
```

### Keywords

host-proxy	IGMP proxy configuration
leave-proxy	IGMP proxy for leave configuration
snooping	Snooping IGMP
ssm-range	IPv4 address range of Source Specific Multicast
unknown-flooding	Flooding unregistered IPv4 multicast traffic

### Parameters

<v_vlan_list>	VLAN identifier(s): VID
<ipv4_mcast>	valid IPv4 multicast address
<ipv4_prefix_length>	Prefix length ranges from 4 to 32

## 6.25 ip name-server Command

### Syntax

```
ip name-server [ <order> ] { <v_ipv4_ucast> | { <v_ipv6_ucast> [ interface vlan
<v_vlan_id_static> ] } | dhcp [ ipv4 | ipv6 ] [ interface vlan <v_vlan_id_dhcp>
```



```
] }
```

### Keywords

interface vlan   vlan interface

dhcp             Dynamic Host Configuration Protocol

### Parameters

<0-3>            Preference of DNS server; Default selection is 0

<ipv4\_ucast>    A valid IPv4 unicast address

<ipv6\_ucast>    A valid IPv6 unicast address

## 6.26 ip route Command

### Syntax

```
ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>
```

### Parameters

<ipv4\_addr>     Network

<ipv4\_netmask>  Subnet mask

<ipv4\_gw>       Default gateway

## 6.27 ip routing Command

To enable Layer 3 IP switching function, use ip routing command.

### Syntax

```
ip routing
```

## 6.28 ip source Command

### Option

```
(config)# ip source ?
```

```
  interface   ip source binding entry interface config
```

### Syntax

```
ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var>  
  <mask_var>
```

### Keywords

interface                    ip source binding entry interface config

### Parameters

<port\_type>                GigabitEthernet, 1 Gigabit Ethernet Port  
<in\_port\_type\_id>        Port ID in 1/1-24  
<vlan\_var>                Select a VLAN id to configure  
<ipv4\_var>                Select an IP Address to configure  
<mask\_var>                Select the subnet mask

## **6.29 ip ssh**

To enable secure shell, ssh, use the ip ssh command.

### Syntax

ip ssh

## **6.30 ip verify source Command**

### Syntax

ip verify source  
ip verify source translate

### Keywords

source            verify source  
translate        ip verify source translate all entries

## **6.31 ipmc Command**

### Options

```
(config)# ipmc ?  
  profile    IPMC profile configuration  
  range     A range of IPv4/IPv6 multicast addresses for the profile
```

### Syntax

```
ipmc profile  
ipmc profile <profile_name>  
ipmc range <entry_name> { <v_ipv4_mcast> [ <v_ipv4_mcast_1> ] | <v_ipv6_mcast>
```

```
[ <v_ipv6_mcast_1> ] }
```

#### Parameters

< profile_name>	Profile name in 16 char's
<entry_name>	Range entry name in 16 char's
<ipv4_mcast>	Valid IPv4 multicast address
<ipv6_mcast>	Valid IPv6 multicast address

## 6.32 ipv6 Command

#### Options

```
(config)# ipv6 ?  
  mld      Multicasat Listener Discovery  
  route    Configure static routes
```

#### Syntax

```
ipv6 mld host-proxy [ leave-proxy ]  
ipv6 mld snooping  
ipv6 mld snooping vlan <v_vlan_list>  
ipv6 mld ssm-range <v_ipv6_mcast> <ipv6_prefix_length>  
ipv6 mld unknown-flooding  
ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan <v_vlan_id>  
  <v_ipv6_addr> }
```

#### Keywords

host-proxy	MLD proxy configuration
snooping	Snooping MLD
ssm-range	IPv6 address range of Source Specific Multicast
unknown-flooding	Flooding unregistered IPv6 multicast traffic
leave-proxy	MLD proxy for leave configuration

#### Parameters

<vlan_list>	VLAN identifier(s): VID
<ipv6_mcast>	Valid IPv6 multicast address
<ipv6_prefix_length>	IPv6 prefix x:x::y/z, X:X:X:X::X/<0-128>
<v_ipv6_subnet>	IPv6 subnet mask
<v_vlan_id>	VID

<v\_ipv6\_addr>                    Valid IPv6 multicast address

## 6.33 json Command

### Option

```
(config)# json ?  
    notification    Notification request object
```

### Syntax

```
json notification host <hname>  
json notification listen <notification> <host>
```

### Parameters

```
<hname>                    <word32> Name of Notification host  
<notification>            <word> Valid words are 'acl.status.ace.crossed-threshold.update'  
                          'aggregation.status.group.update'  
                          'arp-inspection.status.crossed-threshold.update'  
                          'ip.status.interface.dhcp-client.update'  
                          'ip.status.interface.ipv4.update'  
                          'ip.status.interface.ipv6.update'  
                          'ip.status.interface.link.update' 'ip.status.route.ipv4.update'  
                          'ip.status.route.ipv6.update' 'port.status.update'
```

## 6.34 lacp Command

### Option

```
(config)# lacp ?  
    system-priority    System priority
```

### Syntax

```
(config)# lacp ?  
lacp system-priority <v_1_to_65535>
```

## 6.35 line Command

### Options

```
(config)# line ?
```

<0~16> List of line numbers  
console Console terminal line  
vty Virtual terminal

### Syntax

```
line { <0~16> | console 0 | vty <0~15> }
```

### Parameters

0 Console Line number  
<0~15> List of vty numbers

## 6.36 lldp Command

### Options

```
(config)# lldp ?
```

holdtime	Sets LLDP hold time (The neighbor switch will discarded the LLDP information after "hold time" multiplied with "timer" seconds ).
med	Media Endpoint Discovery.
reinit	LLDP tx reinitialization delay in seconds.
timer	Sets LLDP TX interval (The time between each LLDP frame transmitted in seconds).
transmission-delay	Sets LLDP transmission-delay. LLDP transmission delay (the amount of time that the transmission of LLDP frames will delayed after LLDP configuration has changed) in seconds.)

### Syntax

```
lldp holdtime <val>  
lldp med datum { wgs84 | nad83-navd88 | nad83-mllw }  
lldp med fast <v_1_to_10>  
lldp med location-tlv altitude { meters | floors } <v_word11>  
lldp med location-tlv civic-addr { country | state | county | city | district  
| block | street | leading-street-direction | trailing-street-suffix  
| street-suffix | house-no | house-no-suffix | landmark | additional-info | name  
| zip-code | building | apartment | floor | room-number | place-type  
| postal-community-name
```

```

    | p-o-box | additional-code } <v_string250>
lldp med location-tlv elin-addr <v_word25>
lldp med location-tlv latitude { north | south } <v_word8>
lldp med location-tlv longitude { west | east } <v_word9>
lldp med media-vlan-policy <policy_index> { voice | voice-signaling
    | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing
    | streaming-video | video-signaling } { tagged <v_vlan_id> | untagged }
    [ 12-priority <v_0_to_7> ] [ dscp <v_0_to_63> ]
lldp reinit <val>
lldp timer <val>
lldp transmission-delay <val>

```

## 6.37 logging Command

### Options

```

(config)# logging ?
    host      host
    level     level
    on        Enable syslog server

```

### Syntax

```

logging host { <ipv4_ucast> | <domain_name> }
logging level { informational | notice | warning | error }
logging on

```

### Parameters

```

<domain_name>  The domain name is to provide a mechanism for naming
                resources on the Internet. A complete domain name consists
                of one or more subdomain names which are separated by
                dots(.)

<ipv4_ucast>   The IPv4 address of the log server

Error          Severity 3: Error conditions
Informational  Severity 6: Informational messages
Notice        Severity 5: Normal but significant condition
Warning       Severity 4: Warning conditions

```

## 6.38 loop-protect Command

### Options

```
(config)# loop-protect ?  
  shutdown-time    Loop protection shutdown time interval  
  transmit-time    Loop protection transmit time interval  
  <cr>
```

### Syntax

```
(config)# loop-protect ?  
loop-protect  
loop-protect shutdown-time <t>  
loop-protect transmit-time <t>
```

### Parameters

```
<0-604800>  Shutdown time in second  
<1-10>     Transmit time in second
```

## **6.39 mac address-table Command**

```
(config)# mac ?  
  address-table    MAC table entries/configuration
```

### Syntax

```
mac address-table aging-time <v_0_10_to_1000000>  
mac address-table learning vlan <vlan_list>  
mac address-table static <v_mac_addr> vlan <v_vlan_id> interface ( <port_type>  
  [ <v_port_type_list> ] )
```

### Parameters

```
<0,10-1000000> Aging time in seconds, 0 disables aging  
<mac_addr>     48 bit MAC address: xx:xx:xx:xx:xx:xx  
<vlan_list>
```

## **6.40 monitor Command**

### Options

```
(config)# monitor ?
```

**Destination** The destination port. That is the port that trafficed should be mirrored to.

**Source** The source port(s). That is the ports to be mirrored to the destination port.

### Syntax

```
monitor destination interface <port_type> <in_port_type>
monitor source interface { ( <port_type> [ <v_port_type_list> ] ) } { both | rx | tx }
```

### Keywords

**Destination** The destination port. That is the port that trafficed should be mirrored to.

**Source** The source port(s). That is the ports to be mirrored to the destination port.

**Interface** Interface to mirror traffic to.

**\*** All switches or All ports

**GigabitEthernet** 1 Gigabit Ethernet Port

**10GigabitEthernet** 10 Gigabit Ethernet Port

**Both** Setting source port to both will mirror both ingress and egress traffic.

**Rx** Setting source port to rx will mirror ingress traffic.

**Tx** Setting source port to tx will mirror egress traffic.

### Parameters

**<port\_type>** \*, GigabitEthernet, 10GigabitEthernet

**<in\_port\_type>** 1G Port ID in 1/1-24

**<v\_port\_type\_list>** 10G Port list in 1/1-2

## 6.41 mvr Command

### Options

```
(config)# mvr ?
  name    MVR multicast name
  vlan    MVR multicast vlan
  <cr>
```

### Syntax



```

mvr
mvr name <mvr_name> channel <profile_name>
mvr name <mvr_name> frame priority <cos_priority>
mvr name <mvr_name> frame tagged
mvr name <mvr_name> igmp-address <v_ipv4_ucast>
mvr name <mvr_name> last-member-query-interval <ipmc_lmqi>
mvr name <mvr_name> mode { dynamic | compatible }
mvr vlan <v_vlan_list> [ name <mvr_name> ]
mvr vlan <v_vlan_list> channel <profile_name>
mvr vlan <v_vlan_list> frame priority <cos_priority>
mvr vlan <v_vlan_list> frame tagged
mvr vlan <v_vlan_list> igmp-address <v_ipv4_ucast>
mvr vlan <v_vlan_list> last-member-query-interval <ipmc_lmqi>
mvr vlan <v_vlan_list> mode { dynamic | compatible }

```

### Parameters

<mvr_name>	Word16, MVR multicast VLAN name
channel	MVR channel configuration
frame	MVR control frame in TX
priority	Interface CoS priority
tagged	Tagged IGMP/MLD frames will be sent
igmp-address	MVR address configuration used in IGMP
<ipmc_lmqi>	0 - 31744 tenths of seconds
last-member-query-interval	Last Member Query Interval in tenths of seconds
mode	MVR mode of operation
compatible	Compatible MVR operation mode
dynamic	Dynamic MVR operation mode
<vlan_list>	MVR multicast VLAN list

## 6.42 no Command

### Options

```

(config)# no ?
  Aaa           Authentication, Authorization and Accounting
  Access       Access management
  access-list   Access list
  aggregation   Aggregation mode

```

banner	Define a login banner
clock	Configure time-of-day clock
dot1x	IEEE Standard for port-based Network Access Control
enable	Modify enable password parameters
green-ethernet	Green ethernet (Power reduction)
gvrp	Enable GVRP feature
hostname	Set system's network name
interface	Select an interface to configure
ip	Internet Protocol
ipmc	IPv4/IPv6 multicast configuration
ipv6	IPv6 configuration commands
json	Json-rpc related configuration
lACP	LACP settings
lldp	LLDP configurations.
Logging	System logging message
loop-protect	Loop protection configuration
mac	MAC table entries/configuration
monitor	Monitoring different system events
mvr	Multicast VLAN Registration configuration
ntp	Configure NTP
poE	Power Over Ethernet.
port-security	Enable/disable port security globally.
Privilege	Command privilege parameters
QoS	Quality of Service
radius-server	Configure RADIUS
rmon	Remote Monitoring
sflow	Statistics flow.
snmp-server	Enable SNMP server
spanning-tree	STP Bridge
tacacs-server	Configure TACACS+
udld	Disable UDLD configurations on all fiber-optic ports.
UpnP	Set UPnP's configurations
Username	Establish User Name Authentication
Vlan	Vlan commands
Voice	Voice appliance attributes
web	web

## 6.43 ntp Command

### Options

```
(config)# ntp ?  
  server      Configure NTP server  
  <cr>       Enable ntp function
```

### Syntax

```
ntp  
ntp server <index_var> ip-address { <ipv4_var> | <ipv6_var> | <name_var> }
```

### Parameters

```
<index_var>    <1-5> index number  
<hostname>    domain name  
<ipv4_ucast>  ipv4 address  
<ipv6_ucast>  ipv6 address
```

## 6.44 port-security Command

### Options

```
(config)# port-s ?  
  aging      Enable/disable port security aging.  
  <cr>
```

### Syntax

```
port-security  
port-security aging  
port-security aging time <v_10_to_10000000>
```

### Parameters

```
Time          seconds between check for activity on learned MAC addresses.  
<10-10000000> seconds
```

## 6.45 privilege Command

### Syntax

```
(config)# privilege ?
```

privilege <mode\_name> level <privilege> <cmd>

<mode\_name>        <word> valid words are 'config-vlan' 'configure' 'dhcp-pool'  
                      'exec' 'if-vlan' 'interface' 'ipmc-profile' 'json-noti-host'  
                      'line' 'snmps-host' 'stp-aggr'  
level                Set privilege level of command  
<0-15>                Privilege level  
<cmd>                <line128> Initial valid words and literals of the command to modify,  
                      in 128 char's

## 6.46 qos Command

### Options

(config)# qos ?

Map        Global QoS Map/Table  
Qce        QoS Control Entry  
Storm      Storm policer  
wred        Weighted Random Early Discard

(config)# qos map ?

cos-dscp                    Map for cos to dscp  
dscp-classify                Map for dscp classify enable  
dscp-cos                     Map for dscp to cos  
dscp-egress-translation      Map for dscp egress translation  
dscp-ingress-translation      Map for dscp ingress translation

(config)# qos qce ?

<1-256>        QCE ID  
Refresh        Refresh QCE tables in hardware  
Update         Update an existing QCE

(config)# qos storm ?

Broadcast      Police broadcast frames  
Multicast      Police multicast frames  
Unicast        Police unicast frames

(config)# qos wred ?

Group          Specify group

### Syntax

```

qos map cos-dscp <cos> dp1 <dp1> dscp { <dscp_num> | { be | af11 | af12 | af13 |
af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3
| cs4 | cs5 | cs6 | cs7 | ef | va } }
qos map dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | a
f23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs
6 | cs7 | ef | va } }
qos map dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 |
af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | c
s7 | ef | va } } cos <cos> dp1 <dp1>
qos map dscp-egress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21
| af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4
| cs5 | cs6 | cs7 | ef | va } } <dp1> to { <dscp_num_tr> | { be | af11 | af12 |
af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2
| cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }
qos map dscp-ingress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21
| af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4
| cs5 | cs6 | cs7 | ef | va } } to { <dscp_num_tr> | { be | af11 | af12 | af13
| af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3
| cs4 | cs5 | cs6 | cs7 | ef | va } }
qos qce refresh
qos qce { [ update ] } <qce_id> [ { next <qce_id_next> } | last ] [ interface (
<port_type> [ <port_list> ] ) ] [ smac { <smac> | <smac_24> | any } ] [ dmac { <
dmac> | unicast | multicast | broadcast | any } ] [ tag { [ type { untagged | ta
gged | c-tagged | s-tagged | any } ] [ vid { <ot_vid> | any } ] [ pcp { <ot_pcp>
| any } ] [ dei { <ot_dei> | any } ] }*1 ] [ inner-tag { [ type { untagged | ta
gged | c-tagged | s-tagged | any } ] [ vid { <it_vid> | any } ] [ pcp { <it_pcp>
| any } ] [ dei { <it_dei> | any } ] }*1 ] [ frame-type { any | { etype [ { <et
ype_type> | any } ] } | { llc [ dsap { <llc_dsap> | any } ] [ ssap { <llc_ssap>
| any } ] [ control { <llc_control> | any } ] } | { snap [ { <snap_data> | any }
] } | { ipv4 [ proto { <pr4> | tcp | udp | any } ] [ sip { <sip4> | any } ] [ d
ip { <dip4> | any } ] [ dscp { <dscp4> | { be | af11 | af12 | af13 | af21 | af22
| af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5
| cs6 | cs7 | ef | va } | any } ] [ fragment { yes | no | any } ] [ sport { <sp4
> | any } ] [ dport { <dp4> | any } ] } | { ipv6 [ proto { <pr6> | tcp | udp |
any } ] [ sip { <sip6> | any } ] [ dip { <dip6> | any } ] [ dscp { <dscp6> | { be
| af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 |
af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any } ] [ sport { <

```

```

sp6> | any } ] [ dport { <dp6> | any } ] } ] [ action { [ cos { <action_cos>
| default } ] [ dpl { <action_dp1> | default } ] [ pcp-dei { <action_pcp> <action
_dei> | default } ] [ dscp { <action_dscp_dscp> | { be | af11 | af12 | af13 | af
21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 |
cs4 | cs5 | cs6 | cs7 | ef | va } | default } ] [ policy { <action_policy> | defa
ult } ] ] }*1 ]
qos storm { unicast | multicast | broadcast } <rate> [ fps | kfps | kbps | mbps]
qos wred group <group> queue <queue> dpl <dpl> min-fl <min_fl> max <max>
[ fill-level ]

```

### Parameters

<0-63>	Specific DSCP
af11	Assured Forwarding PHB AF11(DSCP 10)
af12	Assured Forwarding PHB AF12(DSCP 12)
af13	Assured Forwarding PHB AF13(DSCP 14)
af21	Assured Forwarding PHB AF21(DSCP 18)
af22	Assured Forwarding PHB AF22(DSCP 20)
af23	Assured Forwarding PHB AF23(DSCP 22)
af31	Assured Forwarding PHB AF31(DSCP 26)
af32	Assured Forwarding PHB AF32(DSCP 28)
af33	Assured Forwarding PHB AF33(DSCP 30)
af41	Assured Forwarding PHB AF41(DSCP 34)
af42	Assured Forwarding PHB AF42(DSCP 36)
af43	Assured Forwarding PHB AF43(DSCP 38)
be	Default PHB(DSCP 0) for best effort traffic
cs1	Class Selector PHB CS1 precedence 1(DSCP 8)
cs2	Class Selector PHB CS2 precedence 2(DSCP 16)
cs3	Class Selector PHB CS3 precedence 3(DSCP 24)
cs4	Class Selector PHB CS4 precedence 4(DSCP 32)
cs5	Class Selector PHB CS5 precedence 5(DSCP 40)
cs6	Class Selector PHB CS6 precedence 6(DSCP 48)
cs7	Class Selector PHB CS7 precedence 7(DSCP 56)
ef	Expedited Forwarding PHB(DSCP 46)
va	oice Admit PHB(DSCP 44)
action	Setup action
dmac	Setup matched DMAC
frame-type	Setup matched frame type

inner-tag	Setup inner tag options
interface	Interfaces
last	Place QCE at the end
next	Place QCE before the next QCE ID
smac	Setup matched SMAC
tag	Setup tag options
cos	Setup class of service action
dpl	Setup drop precedence level action
dscp	Setup DSCP action
pcp-dei	Setup PCP and DEI action
policy	Setup ACL policy action
fps	Unit is frames per second (default)
kbits	Unit is kilobits per second
kfps	Unit is kiloframes per second
mbps	Unit is Megabits per second

## 6.47 radius-server Command

### Options

(config)# radius-server ?

Attribute	NAS attributes
Deadtime	Time to stop using a RADIUS server that doesn't respond
Host	Specify a RADIUS server
Key	Set RADIUS encryption key
Retransmit	Specify the number of retries to active server
Timeout	Time to wait for a RADIUS server to reply

### Syntax

```
radius-server attribute 32 <id>
radius-server attribute 4 <ipv4>
radius-server attribute 95 <ipv6>
radius-server deadtime <minutes>
radius-server host <host_name> [ auth-port <auth_port> ] [ acct-port <acct_port>
] [ timeout <seconds> ] [ retransmit <retries> ] [ key <key> ]
radius-server key <key>
radius-server retransmit <retries>
radius-server timeout <seconds>
```

### Parameters

32                    attribute number 32 = NAS-Identifier  
4                     attribute number 4 = NAS-IP-Address  
95                    attribute number 95 = NAS-IPV6-Address  
<1-1440>            Time in minutes  
<word1-255>        Hostname or IP address  
<1-1440>            Time in minutes  
<word1-255>        Hostname or IP address  
<1-1440>            Time in minutes  
<word1-255>        Hostname or IP address  
<line1-63>          The shared key  
<1-1000>            Number of retries for a transaction  
<1-1000>            wait time in seconds

## 6.48 rmon Command

### Options

```
(config)# rmon ?  
  alarm    Configure an RMON alarm  
  event    Configure an RMON event
```

### Syntax

```
rmon alarm <id> <oid_str> <interval> { absolute | delta } rising-threshold  
  <rising_threshold> [ <rising_event_id> ] falling-threshold <falling_threshold>  
  [ <falling_event_id> ] { [ rising | falling | both ] }  
rmon alarm <id> { ifInOctets | ifInUcastPkts | ifInNUcastPkts | ifInDiscards  
  | ifInErrors | ifInUnknownProtos | ifOutOctets | ifOutUcastPkts | ifOutNUcastPkts  
  | ifOutDiscards | ifOutErrors } <ifIndex> <interval> { absolute | delta }  
  rising-threshold <rising_threshold> [ <rising_event_id> ] falling-threshold  
  <falling_threshold> [ <falling_event_id> ] { [ rising | falling | both ] }  
rmon event <id> [ log ] [ trap <community> ] { [ description <description> ] }
```

### Parameters

<1-65535>            Alarm entry ID  
<oid\_str>            WORD, MIB object to monitor  
<1-2147483647>      Sample interval



absolute	Test each sample directly
delta	Test delta between samples
rising-threshold	Configure the rising threshold <-2147483648-2147483647> rising threshold value
<0-65535>	Event to fire on rising threshold crossing
falling-threshold	Configure the falling threshold <-2147483648-2147483647> falling threshold value
<0-65535>	Event to fire on falling threshold crossing
both	Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default)
falling	Trigger alarm when the first value is less than the falling threshold
rising	Trigger alarm when the first value is larger than the rising threshold
ifInDiscards	The number of inbound packets that are discarded even the packets are normal
ifInErrors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol
ifInNUcastPkts	The number of broad-cast and multi-cast packets delivered to a higher-layer protocol
ifInOctets	The total number of octets received on the interface, including framing characters
ifInUcastPkts	The number of uni-cast packets delivered to a higher-layer protocol
ifInUnknownProtos	The number of the inbound packets that were discarded because of the unknown or un-support protocol
ifOutDiscards	The number of outbound packets that are discarded The packets is normal
ifOutErrors	The The number of outbound packets that could not be transmitted because of errors
ifOutNUcastPkts	The number of broad-cast and multi-cast packets that request to transmit
ifOutOctets	The number of octets transmitted out of the interface , including framing characters
ifOutUcastPkts	The number of uni-cast packets that request to transmit
<1-65535>	Event entry ID

description	Specify a description of the event
log	Generate RMON log when the event fires
trap	Generate SNMP trap when the event fires
<community>	WORD, SNMP community string
<description>	LINE, Event description

## 6.49 sflow Command

### Options

(config)# sflow ?

agent-ip	The agent IP address used as agent-address in UDP datagrams. Defaults to IPv4 loopback address.
collector-address	Collector address
collector-port	Collector UDP port
max-datagram-size	Maximum datagram size.
timeout	Receiver timeout measured in seconds. The switch decrements the timeout once per second, and as long as it is non-zero, the receiver receives samples. Once the timeout reaches 0, the receiver and all its configuration is reset to defaults.

### Syntax

```
sflow agent-ip { ipv4 <v_ipv4_addr> | ipv6 <v_ipv6_addr> }
sflow collector-address [ <host_name> ]
sflow collector-port <collector_port>
sflow max-datagram-size <datagram_size>
sflow timeout [ receiver <rcvr_idx_list> ] <timeout>
```

### Parameters

ipv4	IPv4 address or IPv6 address or hostname identifying the collector receiver
<collector_port>	1-65535, Port number
<datagram_size>	200-1468 bytes
<timeout>	0-2147483647 seconds

## 6.50 snmp-server Command

## Options

(config)# snmp-server ?

access	access configuration
community	Set the SNMP community
contact	Set the SNMP server's contact string
engine-id	Set SNMP engine ID
host	Set SNMP host's configurations
location	Set the SNMP server's location string
security-to-group	Security-to-group configuration
trap	Set trap's configurations
user	Set the SNMPv3 user's configurations
version	Set the SNMP server's version
view	MIB view configuration

## Syntax

```
snmp-server access <group_name> model { v1 | v2c | v3 | any }
    level { auth | noauth | priv } [ read <view_name> ] [ write <write_name> ]
snmp-server community v2c <comm> [ ro | rw ]
snmp-server community v3 <v3_comm> [ <v_ipv4_addr> <v_ipv4_netmask> ]
snmp-server contact <v_line255>
snmp-server engine-id local <engineID>
snmp-server host <conf_name>
snmp-server location <v_line255>
snmp-server security-to-group model { v1 | v2c | v3 } name <security_name>
    group <group_name>
snmp-server trap
snmp-server user <username> engine-id <engineID> [ { md5 <md5_passwd>
    | sha <sha_passwd> } [ priv { des | aes } <priv_passwd> ] ]
snmp-server version { v1 | v2c | v3 }
snmp-server view <view_name> <oid_subtree> { include | exclude }
```

## Parameters

<group_name>	Group Name : word32
model	security model
any	any security model
v1	v1 security model

v2c	v2c security model
v3	v3 security model
auth	authNoPriv Security Level
noauth	noAuthNoPriv Security Level
priv	authPriv Security Level
<view_name>	word255, read view name
read	specify a read view for the group
write	specify a write view for the group
<write_name>	word255, write view name
<comm.>	word255, Community name
ro	Read only
rw	Read write
<v3_comm>	word32, Community name
<v_ipv4_addr>	IPv4 address
<v_line255>	line string
local	Set SNMP local engine ID
<engineID>	word10-32, local engine ID
<conf_name>	Name of the host configuration
<security_name>	word32, security user name
<user_name>	word32, Username
engine-id	engine ID
md5	Set MD5 protocol
sha	Set SHA protocol
<md5_passwd>	word8-32, MD5 password
priv	Set Privacy
aes	Set AES protocol
des	Set DES protocol
<pri_passwd>	word8-32, Set privacy password
group	security group
<group_name>	word32, security group name
<oid_subtree>	word255, MIB view OID
exclude	Excluded type from the view
include	Included type from the view

## 6.51 spanning-tree Command

### Options

(config)# spanning-tree ?

aggregation	Aggregation mode
edge	Edge ports
mode	STP protocol mode
mst	STP bridge instance
recovery	The error recovery timeout
transmit	BPDUs to transmit

### Syntax

```
spanning-tree aggregation
spanning-tree edge bpdu-filter
spanning-tree edge bpdu-guard
spanning-tree mode { stp | rstp | mstp }
spanning-tree mst <instance> priority <prio>
spanning-tree mst <instance> vlan <v_vlan_list>
spanning-tree mst forward-time <fwdtime>
spanning-tree mst max-age <maxage> [ forward-time <fwdtime> ]
spanning-tree mst max-hops <maxhops>
spanning-tree mst name <name> revision <v_0_to_65535>
spanning-tree recovery interval <interval>
spanning-tree transmit hold-count <holdcount>
```

### Parameters

bpdu-filter	Enable BPDU filter (stop BPDU tx/rx)
bpdu-guard	Enable BPDU guard
mstp	Multiple Spanning Tree (802.1s)
rstp	Rapid Spanning Tree (802.1w)
stp	802.1D Spanning Tree
<instance>	instance 0-7 (CIST=0, MST2=1...)
forward-time	Delay between port states
max-age	Max bridge age before timeout
max-hops	MSTP bridge max hop count
name	Name keyword
priority	Priority of the instance
vlan	VLAN keyword
priority	Priority of the instance
vlan	VLAN keyword

<prio>	0-61440, Range in seconds
<vlan_list>	Range of VLANs
<fwdtime>	4-30, Range in seconds
<maxage>	6-40, Range in seconds
<maxhops>	6-40, Hop count range
<name>	word32, Name of the bridge
revision	Revision keyword
<0-65535>	Revision number
<interval>	30-86400, Range in seconds
hold-count	Max number of transmit BPDUs per sec
<holdcount>	1-10 per sec, 6 is default

## 6.52 tacacs-server Command

### Options

(config)# tacacs-server ?

deadtime	Time to stop using a TACACS+ server that doesn't respond
host	Specify a TACACS+ server
key	Set TACACS+ encryption key
timeout	Time to wait for a TACACS+ server to reply

### Syntax

tacacs-server deadtime <minutes>

tacacs-server host <host\_name> [ port <port> ] [ timeout <seconds> ]  
 [ key <key> ]

tacacs-server key <key>

tacacs-server timeout <seconds>

### Parameters

<minutes>	1-1440, Time in minutes
<host_name>	word1-255, Hostname or IP address
key	Server specific key (overrides default)
port	TCP port for TACACS+ server
timeout	Time to wait for this TACACS+ server to reply (overrides default)
<key>	line1-63, The shared key

## 6.53 udld Command

### Options

(config)# udld ?

- Aggressive Enables UDLD in aggressive mode on all fiber-optic ports.
- Enable Enables UDLD in normal mode on all fiber-optic ports.
- Message Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is from 7 to 90 seconds(Currently default message time interval 7 sec is supported).

### Syntax

udld { aggressive | enable | message time-interval <v\_interval> }

### Parameters

- time-interval Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is from 7 to 90 seconds(Currently default message time interval 7 sec is supported).
- <7-90> Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is from 7 to 90 seconds(Currently default message time interval 7 sec is supported).

## **6.54 upnp Command**

### Options

(config)# upnp ?

- advertising-duration Set advertising duration
- ttl Set TTL value

### Syntax

upnp advertising-duration <v\_100\_to\_86400>  
upnp ttl <v\_1\_to\_255>

## **6.55 username Command**

### Syntax

```
username <username> privilege <priv> password encrypted <encry_password>
username <username> privilege <priv> password none
username <username> privilege <priv> password unencrypted <password>
```

### Parameters

<username>	word31, User name allows letters, numbers and underscores
privilege	Set user privilege level
password	Specify the password for the user
encrypted	Specifies an ENCRYPTED password will follow
none	NULL password
unencrypted	Specifies an UNENCRYPTED password will follow
<encry_password>	word4-44, The ENCRYPTED (hidden) user password. Notice the ENCRYPTED password will be decoded by system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally.
<password>	line31, The UNENCRYPTED (Plain Text) user password. Any printable characters including space is accepted. Notice that you have no chance to get the Plain Text password after this command. The system will always display the ENCRYPTED password.

## 6.56 vlan Command

### Options

```
(config)# vlan ?
  <vlan_list>    ISL VLAN IDs 1~4095
  ethertype     Ether type for Custom S-ports
  protocol      Protocol-based VLAN commands
```

### Syntax

```
vlan <vlist>
vlan ethertype s-custom-port <etype>
vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap
  { <oui> | rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } } group <grp_id>
```

### Parameters

s-custom-port	Custom S-ports configuration
---------------	------------------------------



<etype>	Ethertype (Range: 0x0600-0xffff)
eth2	Ethernet-based VLAN commands
llc	LLC-based VLAN group
snap	SNAP-based VLAN group
arp	Ether Type is ARP
at	Ether Type is AppleTalk
ip	Ether Type is IP
ipx	Ether Type is IPX
<oui>	0x0-0xffffffff, SNAP OUI (Range 0x000000 - 0xFFFFFFFF)
rfc-1042	SNAP OUI is rfc-1042
snap-8021h	SNAP OUI is 8021h
<dsap>	0x0-0xff, DSAP (Range: 0x00 - 0xFF)
<ssap>	0x0-0xff, SSAP (Range: 0x00 - 0xFF)
group	Protocol-based VLAN group commands
<grp_id>	<word16> Group Name (Range: 1 - 16 characters)

## 6.57 voice Command

### Options

```
(config)# voice ?
    vlan      vlan for voice traffic
    <cr>      enable
```

### Syntax

```
voice vlan
voice vlan aging-time <aging_time>
voice vlan class { <traffic_class> }
voice vlan oui <oui> [ description <description> ]
voice vlan vid <vid>
```

### Parameters

aging-time	Set secure learning aging time
<aging_time>	10-10000000, Aging time, 10-10000000 seconds
class	Set traffic class
<traffic_class>	0-7, Traffic class value
oui	OUI configuration
<oui>	xx:xx:xx

description	Set description for the OUI
<description>	line32, Description line
vid	Set VLAN ID
<vlan_id>	VLAN ID, 1-4095

## 6.58 web Command

### Syntax

```
(config)# web ?
```

```
web privilege group <group_name> level { [ cro <cro> ] [ crw <crw> ]
    [ sro <sro> ] [ srw <srw> ] }*1
```

### Parameters

group	web privilege group
<group_name>	Valid words are 'Aggregation' 'DHCP' 'Debug' 'Dhcp_Client' 'Diagnostics' 'EEE' 'Green_Ethernet' 'IP2' 'IPMC_Snooping' 'LACP' 'LLDP' 'Loop_Protect' 'MAC_Table' 'MVR' 'Maintenance' 'Mirroring' 'NTP' 'Ports' 'Private_VLANS' 'QoS' 'RPC' 'Security' 'Spanning_Tree' 'System' 'Timer' 'UPnP' 'VCL' 'VLANS' 'Voice_VLAN' 'XXRP' 'sFlow'
level	web privilege group level
cro	Configuration Read-only level
<cro>	0-15
crw	Configuration Read-write level
<crw>	0-15
sro	Status/Statistics Read-only level
<sro>	0-15
srw	Status/Statistics Read-write level
<srw>	0-15

## 7. Port Interface Configuration Commands

---

```
# configure terminal
(config)# interface ?
*                All ports
GigabitEthernet 1 Gigabit Ethernet Port, 1/1 ~ 1/24
vlan             VLAN interface configurations
```

### 7.1 Port Interface Configuration

To enter port interface configuration mode, use configuration interface command.

#### Example to configure all ports:

```
(config)# interface *
(config-if)#
```

#### Example to configure the port #1:

```
(config)# interface GigabitEthernet 1/1
(config-if)#
```

#### Available commands

access-list	Access list
aggregation	Create an aggregation
do	To run exec commands in config mode
dot1x	IEEE Standard for port-based Network Access Control
duplex	Interface duplex
end	Go back to EXEC mode
excessive-restart	Restart backoff algorithm after 16 collisions (No excessive-restart means discard frame after 16 collisions)
exit	Exit from current mode
flowcontrol	Traffic flow control.
frame-length-check	Drop frames with mismatch between EtherType/Length field and actually payload size.
green-ethernet	Green ethernet (Power reduction)
gvrp	Enable GVRP on port(s)
help	Description of the interactive help system
ip	Internet Protocol

ipv6	IPv6 configuration commands
lacp	Enable LACP on this interface
lldp	LLDP configurations.
loop-protect	Loop protection configuration on port
mac	MAC keyword
media-type	Media type.
mtu	Maximum transmission unit
mvr	Multicast VLAN Registration configuration
no	Negate a command or set its defaults
platform	
port-security	Enable/disable port security per interface.
pvlan	Private VLAN
qos	Quality of Service
rmon	Configure Remote Monitoring on an interface
sflow	Statistics flow.
shutdown	Shutdown of the interface.
snmp-server	Set SNMP server's configurations
spanning-tree	Spanning Tree protocol
speed	Configures interface speed. If you use 10, 100, or 1000 keywords with the auto keyword the port will only advertise the specified speeds.
switchport	Switching mode characteristics
udld	UDLD configurations.

## 7.2 (config-if)# access-list

### Options

(config-if)# access-list ?

action	Access list action
logging	Logging frame information. Note: The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.
Mirror	Mirror frame to destination mirror port
policy	Policy
port-state	Re-enable shutdown port that was shutdown by access-list module

rate-limiter	Rate limiter
redirect	Redirect frame to specific port
shutdown	Shutdown incoming port. The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).

#### Syntax

```

access-list action { permit | deny }
access-list logging
access-list mirror
access-list policy <policy_id>
access-list port-state
access-list rate-limiter <rate_limiter_id>
access-list shutdown
access-list { redirect } interface { <port_type> <port_type_id> }

```

#### Parameters

deny	Deny
permit	Permit
<policy_id>	0-255, Policy ID
<rate_limiter_id>	1-16, Rate limiter ID

### **7.3 (config-if)# aggregation**

#### Option

```

(config-if)# aggregation ?
    group    Create an aggregation group

```

#### Syntax

```
aggregation group <v_uint>
```

#### Parameter

```
<v_uint>    The aggregation group id
```

### **7.4 (config-if)# do**

```

(config-if)# do ?
    LINE    execute Exec Command

```

#### Syntax

do <command>

## 7.5 (config-if)# dot1x

### Options

(config-if)# dot1x ?

guest-vlan	Enables/disables guest VLAN
port-control	Sets the port security state.
radius-qos	Enables/disables per-port state of RADIUS-assigned QoS.
radius-vlan	Enables/disables per-port state of RADIUS-assigned VLAN.
re-authenticate	Refresh (restart) 802.1X authentication process.

### Syntax

dot1x guest-vlan

dot1x port-control { force-authorized | force-unauthorized | auto | single |  
multi | mac-based }

dot1x radius-qos

dot1x radius-vlan

dot1x re-authenticate

### Parameters

auto	Port-based 802.1X Authentication
force-authorized	Port access is allowed
force-unauthorized	Port access is not allowed
mac-based	Switch authenticates on behalf of the client
multi	Multiple Host 802.1X Authentication
single	Single Host 802.1X Authentication

## 7.6 (config-if)# duplex

### Options

(config-if)# duplex ?

auto	Auto negotiation of duplex mode.
full	Forced full duplex.
half	Forced half duplex.

### Syntax

```
duplex { half | full | auto [ half | full ] }
```

## 7.7 (config-if)# end

To exit interface configuration mode and go back to EXEC mode, use end command.

### Example:

```
(config-if)# end  
#
```

## 7.8 (config-if)# excessive-restart

To enable Restart backoff algorithm after 16 collisions, use excessive-restart command. (No excessive-restart means discard frame after 16 collisions)

### Example:

```
(config-if)# excessive-restart  
(config-if)#
```

## 7.9 (config-if)# exit

To exit interface configuration mode and go back to global configuration mode, use exit command.

### Example:

```
(config-if)# exit  
(config)#
```

## 7.10 (config-if)# flowcontrol

### Options

```
(config-if)# flowcontrol ?  
  off      Disable flow control.  
  on       Enable flow control.
```

### Syntax

```
flowcontrol { on | off }
```

## 7.11 (config-if)# frame-length-check

To enable frame length check on the interface port(s), use this command.

**Example:**

```
(config-if)# frame-length-check
(config-if)#
```

## 7.12 (config-if)# green-ethernet

### Options

```
(config-if)# green-ethernet ?
```

eee	Powering down of PHYs when there is no traffic.
energy-detect	Enable power saving for ports with no link partner.
short-reach	Enable power saving for ports which is connect to link partner with short cable.
urgent-queues	Enables EEE urgent queue. An urgent queue means that latency is kept to a minimum for traffic going to that queue. Note: EEE power savings will be reduced.

### Syntax

```
green-ethernet eee
green-ethernet eee urgent-queues [ <urgent_queue_range_list> ]
green-ethernet energy-detect
green-ethernet short-reach
```

## 7.13 (config-if)# gvrp

To enable GVRP on the interface port(s), use gvrp command.

**Example:**

```
(config-if)# gvrp
(config-if)#
```

## 7.14 (config-if)# help

To enable help on the interface port(s), use help command.

**Example:**

```
(config-if)# help
(config-if)#
```



## 7.15 (config-if)# ip

### Options

(config-if)# ip ?

```
arp      Address Resolution Protocol
dhcp     Dynamic Host Configuration Protocol
igmp     Internet Group Management Protocol
verify   verify command
```

### Syntax

```
ip arp inspection check-vlan
ip arp inspection logging { deny | permit | all }
ip arp inspection trust
ip dhcp snooping trust
ip igmp snooping filter <profile_name>
ip igmp snooping immediate-leave
ip igmp snooping max-groups <throttling>
ip igmp snooping mrouter
ip verify source
ip verify source limit <cnt_var>
```

### Parameters

inspection	ARP inspection
check-vlan	ARP inspection VLAN mode config
logging	ARP inspection logging mode config
trust	ARP inspection trust config
filter	Access control on IGMP multicast group registration
immediate-leave	Immediate leave configuration
max-groups	IGMP group throttling configuration
mrouter	Multicast router port configuration
<profile_name>	word16, Profile name in 16 char's
<throttling>	1-10, Maximun number of IGMP group registration
source	verify source
limit	limit command
<cnt_var>	0-2, the number of limit

## 7.16 (config-if)# ipv6 mld

### Syntax

```
ipv6 mld snooping filter <profile_name>
ipv6 mld snooping immediate-leave
ipv6 mld snooping max-groups <throttling>
ipv6 mld snooping mrouter
```

### Parameters

filter	Access control on MLD multicast group registration
immediate-leave	Immediate leave configuration
max-groups	MLD group throttling configuration
mrouter	Multicast router port configuration
<profile_name>	word16, Profile name in 16 char's
<throttling>	1-10, Maximun number of IGMP group registration

## **7.17 (config-if)# lacp**

### Options

```
(config-if)# lacp ?
  key          Key of the LACP aggregation
  port-priority LACP priority of the port
  role         Active / Passive (speak if spoken to) role
  timeout      The period between BPDU transmissions
  <cr>        enable
```

### Syntax

```
lacp
lacp key { <v_1_to_65535> | auto }
lacp port-priority <v_1_to_65535>
lacp role { active | passive }
lacp timeout { fast | slow }
```

### Parameters

<v_1_to_65535>	Key value
auto	Choose a key based on port speed
<v_1_to_65535>	Priority value, lower means higher priority
active	Transmit LACP BPDUS continously

passive	wait for neighbour LACP BPDUs before transmitting
fast	Transmit BPDU each second (fast timeout)
slow	Transmit BPDU each 30th second (slow timeout)

## 7.18 (config-if)# lldp

### Options

(config-if)# lldp ?

cdp-aware	Configures if the interface shall be CDP aware (CDP discovery information is added to the LLDP neighbor table)
med	Media Endpoint Discovery.
receive	Enable/Disable decoding of received LLDP frames.
tlv-select	Which optional TLVs to transmit.
transmit	Enable/Disabled transmission of LLDP frames.

### Syntax

```
lldp cdp-aware
lldp med media-vlan policy-list <v_range_list>
lldp med transmit-tlv [ capabilities ] [ location ] [ network-policy ]
lldp med type { connectivity | end-point }
lldp receive
lldp tlv-select { management-address | port-description | system-capabilities
    | system-description | system-name }
lldp transmit
```

### Parameters

media-vlan	Media VLAN assignment.
transmit-tlv	LLDP-MED Location Type Length Value parameter.
policy-list	Assignment of policies.
<v_range_list>	policies list e.g. 1,2, Policies to assign to the interface.
capabilities	Enable transmission of the optional capabilities TLV.
location	Enable transmission of the optional location TLV.
network-policy	Enable transmission of the optional network-policy TLV.
Connectivity	work as connectivity device.
end-point	work as end-point device.
management-address	Enable/Disable transmission of management address.
port-description	Enable/Disable transmission of port description.

system-capabilities Enable/Disable transmission of system capabilities.  
system-description Enable/Disable transmission of system description.  
system-name Enable/Disable transmission of system name.

## 7.19 (config-if)# loop-protect

```
(config-if)# loop-protect ?  
  action      Action if loop detected  
  tx-mode     Actively generate PDUs  
  <cr>       enable
```

### Syntax

```
loop-protect  
loop-protect action { [ shutdown ] [ log ] }*1  
loop-protect tx-mode
```

### Parameters

```
log          Generate log  
shutdown     Shutdown port
```

## 7.20 (config-if)# mac

### Option

```
(config-if)# mac ?  
  address-table  MAC table configuration
```

### Syntax

```
mac address-table learning [ secure ]
```

### Parameters

```
learning     Port learning mode  
secure       Port Secure mode  
<cr>        enable
```

## 7.21 (config-if)# media-type

### Options

```
(config-if)# media-type ?  
  rj45    rj45 interface (copper interface).  
  fiber   fiber interface  
  dual    Dual media interface (cu & fiber interface).
```

#### Syntax

```
media-type { rj45 | fiber | dual }
```

## 7.22 (config-if)# mtu

#### Options

```
(config-if)# mtu ?  
  1518-10240  Maximum frame size in bytes.
```

#### Syntax

```
mtu <max_length>
```

## 7.23 (config-if)# mvr

#### Options

```
(config-if)# mvr ?  
  immediate-leave  Immediate leave configuration  
  name             MVR multicast name  
  vlan            MVR multicast vlan
```

#### Syntax

```
mvr immediate-leave  
mvr name <mvr_name> type { source | receiver }  
mvr vlan <v_vlan_list> type { source | receiver }
```

#### Parameters

```
<mvr_name>  word16, MVR multicast VLAN name  
type        MVR port role configuration  
receiver    MVR receiver port  
source      MVR source port  
<vlan_list> MVR multicast VLAN list, ex. 1,2,..  
type        MVR port role configuration
```

receiver MVR receiver port  
source MVR source port

## 7.24 (config-if)# no

### Options

(config-if)# no ?

access-list	Access list
aggregation	Aggregation keyword
debug	Debugging functions
dot1x	IEEE Standard for port-based Network Access Control
duplex	Set duplex to default.
excessive-restart	Restart backoff algorithm after 16 collisions (No excessive-restart means discard frame after 16 collisions)
flowcontrol	Configure flow control.
frame-length-check	Do not drop frames with mismatch between EtherType/Length field and actually payload size.
green-ethernet	Green ethernet (Power reduction)
gvrp	Enable GVRP on port(s)
ip	Internet Protocol
ipv6	IPv6 configuration commands
lACP	Enable LACP on this interface
lldp	LLDP configurations.
loop-protect	Loop protection configuration on port
mac	MAC keyword
media-type	Set media type to default (dual for dual-media interfaces, rj45 for interfaces only supporting rj45, fiber for interfaces only supporting sfp).
mtu	Maximum transmission unit
mvr	Multicast VLAN Registration configuration
platform	Platform specific commands
port-security	Enable/disable port security per interface.
priority-flowcontrol	Priority Flowcontrol (802.1Qbb)
pvlan	Private VLAN
qos	Quality of Service
rmon	Configure Remote Monitoring on an interface

sflow	Statistics flow.
shutdown	Shutdown of the interface.
snmp-server	Set SNMP server's configurations
spanning-tree	Enable/disable STP on this interface
speed	Configure speed to default.
switchport	Switching mode characteristics
udld	Disable UDLD

### Syntax

```

no access-list logging
no access-list policy
no access-list port-state
no access-list rate-limiter
no access-list shutdown
no access-list { redirect | port-copy }
no aggregation group
no dot1x guest-vlan
no dot1x port-control
no dot1x radius-qos
no dot1x radius-vlan
no duplex
no excessive-restart
no flowcontrol
no frame-length-check
no green-ethernet eee
no green-ethernet energy-detect
no green-ethernet short-reach
no gvrp
no ip arp inspection check-vlan
no ip arp inspection logging
no ip arp inspection trust
no ip dhcp snooping trust
no ip igmp snooping filter
no ip igmp snooping immediate-leave
no ip igmp snooping max-groups
no ip igmp snooping mrouter
no ip verify source

```

```
no ip verify source limit
no ipv6 mld snooping filter
no ipv6 mld snooping immediate-leave
no ipv6 mld snooping max-groups
no ipv6 mld snooping mrouter
no lacp
no lacp key { <v_1_to_65535> | auto }
no lacp port-priority <v_1_to_65535>
no lacp role { active | passive }
no lacp timeout { fast | slow }
no lldp cdp-aware
no lldp med media-vlan policy-list [ <v_range_list> ]
no lldp med transmit-tlv [ capabilities ] [ location ] [ network-policy ]
no lldp med type
no lldp receive
no lldp tlv-select { management-address | port-description | system-capabilities
| system-description | system-name }
no lldp transmit
no loop-protect
no loop-protect action
no loop-protect tx-mode
no mac address-table learning [ secure ]
no media-type
no mtu
no mvr name <mvr_name> type
no mvr vlan <v_vlan_list> type
no platform phy mode
no port-security
no port-security maximum
no port-security violation
no priority-flowcontrol prio <prio>
no pvlan <pvlan_list>
no pvlan isolation
no qos cos
no qos dei
no qos dpl
no qos dscp-classify
```



```
no qos dscp-remark
no qos dscp-translate
no qos map cos-tag cos <cos> dpl <dpl>
no qos map tag-cos pcp <pcp> dei <dei>
no qos pcp
no qos policer
no qos queue-policer queue <queue>
no qos queue-shaper queue <queue>
no qos shaper
no qos storm { unicast | broadcast | unknown }
no qos tag-remark
no qos trust dscp
no qos trust tag
no qos wred-group
no qos wrp
no rmon collection history <id>
no rmon collection stats <id>
no sflow [ <sampler_idx_list> ]
no sflow counter-poll-interval [ <sampler_idx_list> ]
no sflow max-sampling-size [ sampler <sampler_idx_list> ]
no shutdown
no snmp-server host <conf_name> traps
no spanning-tree
no spanning-tree auto-edge
no spanning-tree bpdu-guard
no spanning-tree edge
no spanning-tree link-type
no spanning-tree mst <instance> cost
no spanning-tree mst <instance> port-priority
no spanning-tree restricted-role
no spanning-tree restricted-tcn
no speed
no switchport access vlan
no switchport forbidden vlan
no switchport hybrid acceptable-frame-type
no switchport hybrid allowed vlan
no switchport hybrid egress-tag
```

```
no switchport hybrid ingress-filtering
no switchport hybrid native vlan
no switchport hybrid port-type
no switchport mode
no switchport trunk allowed vlan
no switchport trunk native vlan
no switchport trunk vlan tag native
no switchport vlan ip-subnet <ipv4>
no switchport vlan mac <mac_addr> [ vlan <vlan_id> ]
no switchport vlan protocol group <grp_id> [ vlan <vlan_id> ]
no switchport voice vlan discovery-protocol
no switchport voice vlan mode
no switchport voice vlan security
```

## 7.25 (config-if)# platform

### Options

```
(config-if)# platform ?
```

```
Phy
```

### Syntax

```
platform phy mode { wan | 1g }
```

### Parameters

```
1g      1G mode
wan     WAN mode
```

## 7.26 (config-if)# port-security

### Options

```
(config-if)# port-security ?
```

```
maximum      Maximum number of MAC addresses that can be learned on this
              set of interfaces.
violation     The action involved with exceeding the limit.
<cr>         Enable
```

### Syntax

```
port-security
port-security maximum [ <v_1_to_1024> ]
port-security violation { protect | trap | trap-shutdown | shutdown }
```

#### Parameters

<v_1_to_1024>	Number of addresses
Protect	Don't do anything
Shutdown	Shutdown the port
Trap	Send an SNMP trap
trap-shutdown	Send an SNMP trap and shutdown the port

## **7.27 (config-if)# priority-flowcontrol**

#### Option

```
(config-if)# priority-flowcontrol ?
    prio    Traffic priority-flowcontrol.
```

#### Syntax

```
priority-flowcontrol prio <prio>
```

#### Parameters

<0~7> Specify range of priorities

## **7.28 (config-if)# pvlan**

#### Option

```
(config-if)# pvlan ?
    <range_list>  list of PVLANS. Range is from 1 to number of ports.
    isolation      Port isolation
```

#### Syntax

```
pvlan <pvlan_list>
pvlan isolation
```

## **7.29 (config-if)# qos**

#### Options

(config-if)# qos ?

cos	Class of service configuration
dei	Drop Eligible Indicator configuration
dpl	Drop precedence level configuration
dscp-classify	DSCP ingress classification
dscp-remark	DSCP egress remarking
dscp-translate	DSCP ingress translation
map	QoS Map/Table configuration
pcp	Priority Code Point configuration
policer	Policer configuration
queue-policer	Queue policer configuration
queue-shaper	Queue shaper configuration
shaper	Shaper configuration
storm	Storm policer
tag-remark	Tag remarking configuration
trust	Trust configuration
wred-group	WRED group configuration
wrr	Weighted round robin configuration

### Syntax

qos cos <cos>

qos dei <dei>

qos dpl <dpl>

qos dscp-classify { zero | selected | any }

qos dscp-remark { rewrite | remap | remap-dp }

qos dscp-translate

qos map cos-tag cos <cos> dpl <dpl> pcp <pcp> dei <dei>

qos map tag-cos pcp <pcp> dei <dei> cos <cos> dpl <dpl>

qos pcp <pcp>

qos policer <rate> [ kbps | mbps | fps | kfps ] [ flowcontrol ]

qos queue-policer queue <queue> <rate> [ kbps | mbps ]

qos queue-shaper queue <queue> <rate> [ kbps | mbps ] [ excess ] [ rate-type { line | data } ]

qos shaper <rate> [ kbps | mbps ] [ rate-type { line | data } ]

qos storm { unicast | broadcast | unknown } <rate> [ fps | kfps | kbps | mbps ]

qos tag-remark { pcp <pcp> dei <dei> | mapped }

qos trust dscp

```
qos trust tag
qos wred-group <wred_group>
qos wrr <w0> <w1> [ <w2> [ <w3> [ <w4> [ <w5> [ <w6> [ <w7> ] ] ] ] ] ] ] ] ] ]
```

Parameters

<cos>	0-7, Specific class of service
<dp1>	0-1, Specific drop precedence level
any	Classify to new DSCP always
selected	Classify to new DSCP if classify is enabled for specific DSCP value in global dscp-classify map
zero	Classify to new DSCP if DSCP is 0
remap	Rewrite DSCP field using classified DSCP remapped through global dscp-egress-translation map
rewrite	Rewrite DSCP field with classified DSCP value (no translation)
cos	Specify class of service
<pcp>	0-7, Specific PCP
<dei>	0-1, Specific DEI
<rate>	100-13200000, Policer rate (default kbps)
<queue>	0~7, Specific queue or range
<rate>	100-13200000, Shaper rate in kbps
excess	Allow use of excess bandwidth
<rate>	100-13200000, Shaper rate in kbps
broadcast	Police broadcast frames
unicast	Police unicast frames
unknown	Police unknown (flooded) frames
fps	Rate is fps
flowcontrol	Enable flow control
mapped	Used mapped values (cos,dp1 -> pcp,dei)
dscp	DSCP value
<w0>	1-100, weight for queue 0
<w1>	1-100, weight for queue 1
<w2>	1-100, weight for queue 2
<w3>	1-100, weight for queue 3
<w4>	1-100, weight for queue 4
<w5>	1-100, weight for queue 5

### 7.30 (config-if)# rmon

## Option

(config-if)# rmon ?

collection     Configure Remote Monitoring Collection on an interface

## Syntax

rmon collection history <id> [ buckets <buckets> ] [ interval <interval> ]  
rmon collection stats <id>

## Parameters

history        Configure history  
<id>           1-65535, History entry ID  
buckets        Requested buckets of intervals. Default is 50 buckets  
<1-65535>      Requested buckets of intervals  
interval       Interval to sample data for each bucket. Default is 1800  
                seconds  
<1-3600>      Interval in seconds to sample data for each bucket  
stats          Configure statistics  
<1-65535>      Statistics entry ID

## **7.31 (config-if)# sflow**

### Options

(config-if)# sflow ?

counter-poll-interval     The interval - in seconds - between counter poller samples.  
max-sampling-size         Specifies the maximum number of bytes to transmit per flow sample.  
sampling-rate             Specifies the statistical sampling rate. The sample rate is specified as N to sample 1/Nth of the packets n the monitored flows. There are no restrictions on the value, but the switch will adjust it to the closest possible sampling rate.  
<cr>                      enable

### Syntax

sflow

```
sflow counter-poll-interval [ <poll_interval> ]
sflow max-sampling-size [ <max_sampling_size> ]
sflow sampling-rate [ <sampling_rate> ]
```

#### Parameters

```
<sampling_rate>      1-4294967295, Sampling rate
<max_sampling_size> 14-200, bytes
```

## 7.32 (config-if)# shutdown

#### Option

```
(config-if)# shutdown
```

#### Syntax

```
shutdown
```

## 7.33 (config-if)# snmp-server

#### Option

```
(config-if)# snmp-server ?
    host    Set SNMP host's configurations
```

#### Syntax

```
snmp-server host <conf_name> traps [ linkup ] [ linkdown ] [ llDP ]
```

#### Parameters

```
<conf_name>      word32, Name of the host configuration
traps            Enable traps
linkdown        Link down event
linkup          Link up event
llDP            LLDP event
```

## 7.34 (config-if)# spanning-tree

#### Options

```
(config-if)# spanning-tree ?
    auto-edge      Auto detect edge status
```

bpdu-guard	Enable/disable BPDU guard
edge	Edge port
link-type	Port link-type
mst	STP bridge instance
restricted-role	Port role is restricted (never root port)
restricted-tcn	Restrict topology change notifications
<cr>	Enable

### Syntax

```
spanning-tree
spanning-tree auto-edge
spanning-tree bpdu-guard
spanning-tree edge
spanning-tree link-type { point-to-point | shared | auto }
spanning-tree mst <instance> cost { <cost> | auto }
spanning-tree mst <instance> port-priority <prio>
spanning-tree restricted-role
spanning-tree restricted-tcn
```

### Parameters

auto	Auto detect
point-to-point	Forced to point-to-point
shared	Forced to Shared
<instance>	instance 0-7 (CIST=0, MST2=1...)
cost	STP Cost of this port
<cost>	1-200000000, Cost range
auto	Use auto cost
port-priority	STP priority of this port
<prio>	0-240, Range (lower higher priority)

## **7.35 (config-if)# speed**

### Options

```
(config-if)# speed ?
  10      10Mbps
  100     100Mbps
  1000    1Gbps
```



10g	10Gbps
2500	2.5Gbps
auto	Auto negotiation

### Syntax

```
speed { 10g | 2500 | 1000 | 100 | 10 | auto { [ 10 ] [ 100 ] [ 1000 ] [ 10g ] } }
```

## 7.36 (config-if)# switchport

### Options

(config-if)# switchport ?

access	Set access mode characteristics of the interface
forbidden	Adds or removes forbidden VLANs from the current list of forbidden VLANs
hybrid	Change PVID for hybrid port
mode	Set mode of the interface
trunk	Change PVID for trunk port
vlan	VLAN commands
voice	Voice appliance attributes

### Syntax

```
switchport access vlan <pvid>
switchport forbidden vlan { add | remove } <vlan_list>
switchport hybrid acceptable-frame-type { all | tagged | untagged }
switchport hybrid allowed vlan { all | none | [ add | remove | except ] <vlan_list> }
switchport hybrid egress-tag { none | all [ except-native ] }
switchport hybrid ingress-filtering
switchport hybrid native vlan <pvid>
switchport hybrid port-type { unaware | c-port | s-port | s-custom-port }
switchport mode { access | trunk | hybrid }
switchport trunk allowed vlan
    { all | none | [ add | remove | except ] <vlan_list> }
switchport trunk native vlan <pvid>
switchport trunk vlan tag native
switchport vlan ip-subnet id <vce_id> <ipv4> vlan <vid>
```

```

switchport vlan mac <mac_addr> vlan <vid>
switchport vlan protocol group <grp_id> vlan <vid>
switchport voice vlan discovery-protocol { oui | lldp | both }
switchport voice vlan mode { auto | force | disable }
switchport voice vlan security

```

### Parameters

vlan	Set VLAN when interface is in access mode
<pvid>	VLAN ID of the VLAN when this port is in access mode
vlan	Add or modify VLAN entry in forbidden table.
add	Add to existing list.
remove	Remove from existing list.
<vlan_list>	VLAN IDs
acceptable-frame-type	Set acceptable frame type on a port
all	Allow all frames
tagged	Allow only tagged frames
untagged	Allow only untagged frames
allowed	Set allowed VLAN characteristics when interface is in hybrid mode
vlan	Set allowed VLANs when interface is in hybrid mode
<vlan_list>	VLAN IDs of the allowed VLANs when this port is in hybrid mode
add	Add VLANs to the current list
all	All VLANs
except	All VLANs except the following
none	No VLANs
remove	Remove VLANs from the current list
egress-tag	Egress VLAN tagging configuration
none	No egress tagging
all	Tag all frames
except-native	Tag all frames except frames classified to native VLAN of the hybrid port
ingress-filtering	VLAN Ingress filter configuration
native	Set native VLAN
port-type	Set port type

## 7.37 (config-if)# udd

## Options

(config-if)# udld ?

port UDLD configuration on port(s)

## Syntax

udld port [ aggressive ] [ message time-interval <v\_interval> ]

## Parameters

Aggressive	Enable UDLD in the aggressive mode on an interface
message	Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is from 7 to 90 seconds(Currently default message time interval 7 sec is supported).
time-interval	Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is from 7 to 90 seconds(Currently default message time interval 7 sec is supported).
<7-90>	Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is from 7 to 90 seconds(Currently default message time interval 7 sec is supported).

## 8. VLAN Interface Configuration Commands

---

```
# configure terminal
(config)# interface ?
    *                All ports
    GigabitEthernet 1 Gigabit Ethernet Port, 1/1 ~ 1/24
    vlan             VLAN interface configurations
```

### 8.1 VLAN Interface Configuration

To enter vlan interface configuration mode, use configuration interface command.

**Example to configure all ports:**

```
(config)# interface *
(config-if)#
```

**Example to configure the VLAN 1:**

```
(config)# interface vlan 1
(config-if-vlan)#
```

**Available commands**

```
(config-if-vlan)# ?
do          To run exec commands in config mode
end         Go back to EXEC mode
exit       Exit from current mode
help       Description of the interactive help system
ip         Interface Internet Protocol config commands
ipv6      IPv6 configuration commands
no        Negate a command or set its defaults
```

### 8.2 (config-if-vlan)# do

```
(config-if-vlan)# do ?
    LINE    execute Exec Command
```

Syntax

```
do <command>
```

### 8.3 (config-if-vlan)# end

To exit interface configuration mode and go back to EXEC mode, use end command.

**Example:**

```
(config-if-vlan)# end
#
```

### 8.4 (config-if-vlan)# exit

To exit vlan interface configuration mode and go back to global configuration mode, use exit command.

**Example:**

```
(config-if-vlan)# exit
(config)#
```

### 8.5 (config-if-vlan)# help

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?').

### 8.6 (config-if-vlan)# ip

Options

```
(config-if-vlan)# ip ?
  address      Address configuraton
  dhcp         Configure DHCP server parameters
  igmp         Internet Group Management Protocol
```

Syntax

```
ip address { { <address> <netmask> } | { dhcp [ fallback <fallback_address>
```

```

    <fallback_netmask> [ timeout <fallback_timeout> ] ] } }
ip dhcp server
ip igmp snooping
ip igmp snooping compatibility { auto | v1 | v2 | v3 }
ip igmp snooping last-member-query-interval <ipmc_lmqi>
ip igmp snooping priority <cos_priority>
ip igmp snooping querier { election | address <v_ipv4_ucast> }
ip igmp snooping query-interval <ipmc_qi>
ip igmp snooping query-max-response-time <ipmc_qri>
ip igmp snooping robustness-variable <ipmc_rv>
ip igmp snooping unsolicited-report-interval <ipmc_uri>

```

### Parameters

<address>	IP address
<netmask>	IP netmask
dhcp	Enable DHCP
fallback	DHCP fallback settings
<fallback_address>	DHCP fallback address
<fallback_netmask>	DHCP fallback netmask
<fallback_timeout>	DHCP fallback timeout in seconds
compatibility	Interface compatibility
auto	Compatible with IGMPv1/IGMPv2/IGMPv3
v1	Forced IGMPv1
v2	Forced IGMPv2
v3	Forced IGMPv3
last-member-query-interval	Last Member Query Interval in tenths of seconds
<ipmc_lmqi>	0 - 31744 tenths of seconds
priority	Interface CoS priority
<cos_priority>	0-7, CoS priority ranges from 0 to 7
querier	IGMP Querier configuration
address	IGMP Querier address configuration
election	Act as an IGMP Querier to join Querier-Election
query-interval	Query Interval in seconds
<ipmc_qi>	1 - 31744 seconds
query-max-response-time	Query Response Interval in tenths of seconds
<ipmc_qri>	0 - 31744 tenths of seconds
robustness-variable	Robustness Variable

<ipmc_rv>	Packet loss tolerance count from 1 to 255
unsolicited-report-interval	Unsolicited Report Interval in seconds
<ipmc_uri>	0 - 31744 seconds

## 8.7 (config-if-vlan)# ipv6

### Options

(config-if-vlan)# ipv6 ?

address	Configure the IPv6 address of an interface
mld	Multicast Listener Discovery

### Syntax

```

ipv6 address <subnet>
ipv6 mld snooping
ipv6 mld snooping compatibility { auto | v1 | v2 }
ipv6 mld snooping last-member-query-interval <ipmc_lmqi>
ipv6 mld snooping priority <cos_priority>
ipv6 mld snooping querier election
ipv6 mld snooping query-interval <ipmc_qi>
ipv6 mld snooping query-max-response-time <ipmc_qri>
ipv6 mld snooping robustness-variable <ipmc_rv>
ipv6 mld snooping unsolicited-report-interval <ipmc_uri>

```

### Parameters

X:X:X:X::X/<0-128>	IPv6 prefix x:x::y/z
auto	Compatible with MLDv1/MLDv2
v1	Forced MLDv1
v2	Forced MLDv2
last-member-query-interval <ipmc_lmqi>	Last Member Query Interval in tenths of seconds 0 - 31744 tenths of seconds
priority <cos_priority>	Interface CoS priority 0-7, CoS priority ranges from 0 to 7
querier address	IGMP Querier configuration IGMP Querier address configuration
election query-interval <ipmc_qi>	Act as an IGMP Querier to join Querier-Election Query Interval in seconds 1 - 31744 seconds

query-max-response-time	Query Response Interval in tenths of seconds
<ipmc_qri>	0 - 31744 tenths of seconds
robustness-variable	Robustness Variable
<ipmc_rv>	Packet loss tolerance count from 1 to 255
unsolicited-report-interval	Unsolicited Report Interval in seconds
<ipmc_uri>	0 - 31744 seconds

## 8.8 (config-if-vlan)# no

To disable a specific function or restore default setting, use no command.

### Options

```

no ip address
no ip dhcp server
no ip igmp snooping
no ip igmp snooping compatibility
no ip igmp snooping last-member-query-interval
no ip igmp snooping priority
no ip igmp snooping querier { election | address }
no ip igmp snooping query-interval
no ip igmp snooping query-max-response-time
no ip igmp snooping robustness-variable
no ip igmp snooping unsolicited-report-interval
no ipv6 address [ <ipv6_subnet> ]
no ipv6 mld snooping
no ipv6 mld snooping compatibility
no ipv6 mld snooping last-member-query-interval
no ipv6 mld snooping priority
no ipv6 mld snooping querier election
no ipv6 mld snooping query-interval
no ipv6 mld snooping query-max-response-time
no ipv6 mld snooping robustness-variable
no ipv6 mld snooping unsolicited-report-interval

```