



# **PDS-408G Commands Line Reference Guide**

06-0014-021



Microsemi Headquarters

One Enterprise, Aliso Viejo, CA 92656 USA

Within the USA: +1 (800) 713-4113

Outside the USA: +1 (949) 380-6100

Sales: +1 (949) 380-6136

Fax: +1 (949) 215-4996

Email: [sales.support@microsemi.com](mailto:sales.support@microsemi.com)

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

© 2019 Microsemi. All rights reserved. Microsemi and the Microsemi logo are trademarks of Microsemi Corporation. All other trademarks and service marks are the property of their respective owners.

Microsemi makes no warranty, representation, or guarantee regarding the information contained herein or the suitability of its products and services for any particular purpose, nor does Microsemi assume any liability whatsoever arising out of the application or use of any product or circuit. The products sold hereunder and any other products sold by Microsemi have been subject to limited testing and should not be used in conjunction with mission-critical equipment or applications. Any performance specifications are believed to be reliable but are not verified, and Buyer must conduct and complete all performance and other testing of the products, alone and together with, or installed in, any end-products. Buyer shall not rely on any data and performance specifications or parameters provided by Microsemi. It is the Buyer's responsibility to independently determine suitability of any products and to test and verify the same. The information provided by Microsemi hereunder is provided "as is, where is" and with all faults, and the entire risk associated with such information is entirely with the Buyer. Microsemi does not grant, explicitly or implicitly, to any party any patent rights, licenses, or any other IP rights, whether with regard to such information itself or anything described by such information. Information provided in this document is proprietary to Microsemi, and Microsemi reserves the right to make any changes to the information in this document or to any products and services at any time without notice.

Microsemi, a wholly owned subsidiary of Microchip Technology Inc. (Nasdaq: MCHP), offers a comprehensive portfolio of semiconductor and system solutions for aerospace & defense, communications, data center and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; enterprise storage and communication solutions; security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, California, and has approximately 4,800 employees globally. Learn more at [www.microsemi.com](http://www.microsemi.com)

# Table of Contents

<b>1.</b>	<b>COMMAND LINE INTERFACE</b> .....	<b>1</b>
1.1.	Completing a partial command.....	1
1.2.	Command History.....	1
<b>2.</b>	<b>GENERAL MAINTENANCE COMMANDS</b> .....	<b>2</b>
2.1.	configure terminal.....	2
2.2.	interface.....	2
2.3.	exit.....	3
2.4.	end.....	3
2.5.	show running-config .....	4
2.6.	show running-config all-default.....	4
2.7.	dir.....	4
2.8.	copy running-config startup-config.....	5
2.9.	copy running-config flash:<file-name> .....	5
2.10.	del flash:<file-name> .....	5
2.11.	reload cold.....	6
2.12.	reload defaults.....	6
2.13.	reload defaults keep-ip .....	6
2.14.	show version.....	7
<b>3.</b>	<b>NETWORK</b> .....	<b>8</b>
3.1.	Ethernet ports - configuration commands .....	8
3.1.1.	<i>Shutdown</i> .....	8
3.1.2.	<i>Speed</i> .....	9
3.1.3.	<i>Duplex</i> .....	10
3.1.4.	<i>flowcontrol</i> .....	11
3.1.5.	<i>MTU</i> .....	11
3.2.	Ethernet ports - view commands.....	12
3.2.1.	<i>Show interface status</i> .....	12
3.3.	IPv4, IPv6 – configuration commands.....	13
3.3.1.	<i>ip name-server - DNS Server</i> .....	13
3.3.2.	<i>ip (ipv6) address - IPv4,IPv6 interface</i> .....	14
3.3.3.	<i>IP Routes (Default gateway)</i> .....	15
3.4.	IPv4, IPv6 – view commands .....	15
3.4.1.	<i>Show interface vlan</i> .....	15
3.5.	NTP (Network Time Protocol) – configuration commands .....	16
3.5.1.	<i>ntp server - Configure NTP server</i> .....	16
3.6.	NTP (Network Time Protocol) – view commands.....	16
3.6.1.	<i>show ntp status - view NTP status</i> .....	16
3.7.	Time Zone – configuration commands .....	17
3.7.1.	<i>clock timezone - time zone configuration</i> .....	17
3.8.	clock summer-time - Daylight Savings Time configuration.....	18
3.9.	Time zone - view commands.....	19
3.9.1.	<i>show clock detail</i> .....	19

3.10.	SysLog report – configuration commands.....	19
3.10.1.	<i>logging - Enable and configure SysLog</i> .....	19
3.11.	SysLog report – view commands .....	20
3.11.1.	<i>show logging</i> .....	20
3.12.	MAC Table Learning – configuration commands .....	20
3.12.1.	<i>mac address-table aging-time</i> .....	21
3.12.2.	<i>mac address-table learning</i> .....	21
3.12.3.	<i>mac address-table static</i> .....	22
3.13.	MAC Table Learning – view commands.....	23
3.13.1.	<i>show mac address-table</i> .....	23
3.14.	Routing – view commands .....	24
3.14.1.	<i>show ip route</i> .....	24
<b>4.</b>	<b>ACCESS CONTROL .....</b>	<b>25</b>
4.1.	Local Users - configuration commands.....	25
4.1.1.	<i>username -Add local user or change password</i> .....	25
4.2.	Local Users - view commands .....	26
4.2.1.	<i>show user-privilege</i> .....	26
4.2.2.	<i>show users</i> ← <i>New command, need to update TOC</i> .....	26
4.3.	Web Server - configuration commands.....	26
4.3.1.	<i>ip http secure-server</i> .....	27
4.3.2.	<i>ip http secure-certificate</i> .....	27
4.4.	Web Server - view commands .....	28
4.4.1.	<i>show ip http</i> .....	28
4.5.	Telnet/SSH/Web - configuration commands.....	28
4.5.1.	<i>aaa authentication login</i> .....	29
4.5.2.	<i>aaa accounting</i> .....	30
4.6.	Telnet/SSH/Web - view commands.....	31
4.6.1.	<i>show aaa</i> .....	31
4.7.	Access Control List - configuration commands.....	32
4.7.1.	<i>access management</i> .....	32
4.8.	Access Control List - view commands.....	33
4.8.1.	<i>show access management</i> .....	33
<b>5.</b>	<b>VLAN .....</b>	<b>34</b>
5.1.	VLAN configuration commands and port types.....	34
5.1.1.	<i>vlan - create VLAN</i> .....	35
5.1.2.	<i>vlan ethertype s-custom-port</i> .....	36
5.1.3.	<i>switchport mode</i> .....	36
5.1.4.	<i>switchport trunk native vlan</i> .....	37
5.1.5.	<i>switchport trunk vlan tag native</i> .....	37
5.1.6.	<i>switchport trunk allowed vlan</i> .....	38
5.1.7.	<i>switchport forbidden vlan</i> .....	39
5.1.8.	<i>switchport hybrid native vlan</i> .....	39
5.1.9.	<i>switchport hybrid port-type</i> .....	40
5.1.10.	<i>switchport hybrid ingress-filtering</i> .....	41

5.1.11.	<i>switchport hybrid acceptable-frame-type</i>	41
5.1.12.	<i>switchport hybrid egress-tag</i>	42
5.1.13.	<i>switchport trunk allowed vlan</i>	43
5.2.	View VLAN Members	44
5.2.1.	<i>show vlan</i>	44
5.3.	View VLAN Ports	44
5.3.1.	<i>show vlan status</i>	44
<b>6.</b>	<b>POE-BT POWER</b>	<b>45</b>
6.1.	PoE-BT Power configuration commands	45
6.1.1.	<i>poe extended-bt-power-mode</i>	45
6.1.2.	<i>poe uninterruptible-power</i>	45
6.1.3.	<i>poe power</i>	46
6.1.4.	<i>poe mode</i>	46
6.1.5.	<i>poe priority</i>	47
6.1.6.	<i>poe terminal-description</i>	47
6.2.	PoE-BT Power view commands	48
6.2.1.	<i>show poe</i>	48
<b>7.</b>	<b>SPANNING TREE</b>	<b>49</b>
7.1.	STP Bridge Configuration commands	49
7.1.1.	<i>spanning-tree mode</i>	49
7.1.2.	<i>spanning-tree system settings</i>	49
7.1.3.	<i>spanning-tree port settings</i>	51
7.2.	STP Bridges view commands	52
7.2.1.	<i>show spanning-tree</i>	52
<b>8.</b>	<b>SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)</b>	<b>53</b>
8.1.	Enable/Disable SNMP and configure MIB-II system OIDs	53
8.1.1.	<i>snmp-server</i>	53
8.1.2.	<i>snmp-server contact, System-Name (host) and location</i>	54
8.2.	SNMPv2-v3 Configuration commands	55
8.2.1.	<i>snmp-server view</i>	55
8.2.2.	<i>snmp-server community</i>	55
8.2.3.	<i>snmp-server user</i>	56
8.2.4.	<i>snmp-server security-to-group model</i>	56
8.2.5.	<i>snmp-server access</i>	57
8.2.6.	<i>snmp-server trap</i>	57
8.2.7.	<i>snmp-server host</i>	58
8.3.	SNMP view commands	59
8.3.1.	<i>show snmp</i>	59
<b>9.</b>	<b>RADIUS TACACS+</b>	<b>60</b>
9.1.	RADIUS Server configuration commands	60
9.1.1.	<i>Global configuration commands</i>	60
9.1.2.	<i>Radius server configuration</i>	61
9.2.	RADIUS Server Status view commands	61
9.2.1.	<i>show radius-server</i>	61

9.3.	TACACS+ Server configuration commands .....	62
9.3.1.	Global configuration commands.....	62
9.3.2.	TACACS+ Server configuration.....	63
9.4.	TACACS+ Server view commands.....	63
9.4.1.	show tacacs-server .....	63
<b>10.</b>	<b>AGGREGATION/LACP .....</b>	<b>64</b>
10.1.	Aggregation Group Configuration commands.....	64
10.1.1.	aggregation mode .....	64
10.1.2.	aggregation group .....	65
10.1.3.	lacp failover .....	65
10.1.4.	lacp max-bundle .....	66
10.2.	Aggregation Group Status view commands.....	66
10.2.1.	show aggregation .....	66
10.3.	LACP Configuration commands .....	67
10.3.1.	lacp system-priority .....	67
10.3.2.	lacp port-priority.....	67
10.3.3.	lacp timeout .....	68
10.4.	LACP View commands.....	68
10.4.1.	show lacp system-id .....	68
10.4.2.	show lacp internal details .....	69
10.4.3.	show lacp neighbor details.....	69
10.4.4.	show lacp statistics details .....	69
<b>11.</b>	<b>LLDP (LINK LAYER DISCOVERY PROTOCOL) .....</b>	<b>70</b>
11.1.	LLDP Configuration commands .....	70
11.1.1.	LLDP parameters .....	70
11.1.2.	LLDP Interface configuration.....	71
11.2.	LLDP View commands .....	72
11.2.1.	show lldp neighbors.....	72
11.2.2.	show lldp statistics.....	72
<b>12.</b>	<b>PRIVATE VLAN / PORT ISOLATION .....</b>	<b>73</b>
12.1.	Private VLAN configuration commands .....	73
12.1.1.	pvlan.....	73
12.2.	Private VLAN view commands .....	73
12.2.1.	show pvlan .....	73
12.3.	Port Isolation configuration commands .....	74
12.3.1.	pvlan isolation.....	74
12.4.	Port Isolation view commands.....	74
12.4.1.	show pvlan isolation .....	74
<b>13.</b>	<b>LOOP PROTECTION .....</b>	<b>75</b>
13.1.	Loop protection configuration commands .....	75
13.1.1.	loop-protect (general settings) .....	75
13.1.2.	loop-protect (port settings) .....	76
13.2.	Loop protection status view commands .....	76
13.2.1.	show loop-protect.....	76

<b>14.</b>	<b>IGMP (INTERNET GROUP MANAGEMENT PROTOCOL)</b> .....	<b>77</b>
14.1.	IGMP Snooping Configuration commands .....	77
14.1.1.	<i>ip igmp (global parameters)</i> .....	77
14.1.2.	<i>ip igmp snooping (port parameters)</i> .....	78
14.1.3.	<i>ip igmp snooping (vlan parameters)</i> .....	79
14.2.	IGMP Snooping View commands .....	80
14.2.1.	<i>show ip igmp snooping group-database</i> .....	80
14.2.2.	<i>show ip igmp snooping mrouter</i> .....	80
<b>15.</b>	<b>PORT MIRRORING</b> .....	<b>81</b>
15.1.	Port mirroring configuration .....	81
15.1.1.	<i>monitor session</i> .....	81
15.1.2.	<i>Port configuration</i> .....	82
<b>16.</b>	<b>MAINTENANCE</b> .....	<b>83</b>
16.1.	Reset and Restore unit .....	83
16.1.1.	<i>reload cold</i> .....	83
16.1.2.	<i>reload defaults keep-ip</i> .....	83
16.1.3.	<i>reload defaults</i> .....	84
16.2.	Unit Configuration .....	84
16.2.1.	<i>Download unit configuration to TFTP-Server</i> .....	84
16.2.2.	<i>Upload configuration file from TFTP-Server to unit</i> .....	85
16.2.3.	<i>Activate one of the already stored configuration files</i> .....	86
16.2.4.	<i>Delete configuration</i> .....	86
16.3.	Software update .....	86
16.3.1.	<i>Upload new version</i> .....	86
16.3.2.	<i>Select active Image</i> .....	87
<b>17.</b>	<b>DIAGNOSTICS</b> .....	<b>88</b>
17.1.	View log file .....	88
17.2.	Ping .....	88
17.3.	RJ45 Cable test .....	89
17.4.	View CPU Load .....	90

# 1. COMMAND LINE INTERFACE

Command-line interface (CLI) is used for configuring, monitoring, and maintaining PDS-408G/F/M/AC switch over CLI, Telnet, SSH. Please use baud rate of **115200** whenever using the front panel USB serial interface.



## NOTE:

**Note-1: it is strongly recommended to use the Web interface whenever possible to simplify user configuration and reduce configuration mismatch.**

**Note-2: CLI interface may contain more configuration commands Vs those affected as a result of user configuration changes over the web. This manual covers only the commands affected whenever user change unit configuration over the Web interface.**

All commands entered in CLI are followed by values, parameters or both. Parameters may be mandatory values, optional values, choices, or a combination.

**<parameter>**. The < > angle brackets indicate that a mandatory parameter is to be entered in place of the brackets and text inside them.

**[parameter]**. The [ ] square brackets indicate that an optional parameter may be entered in place of the brackets and text inside them.

**choice1 | choice2**. The | indicates that only one of the parameters should be entered.

The { } curly braces indicate that a parameter must be chosen from the list of choices.

Values may be in a form of six hexadecimal numbers separated by colons (MAC address), for example 00:06:29:32:81:40., dotted-decimal notation (Area IDs), for example 0.0.0.1 , slot/port number for example 1/1 or logical slot/port (applicable in case of a link-aggregation).

## 1.1. Completing a partial command

Enter the first few letters of the command, and then press the Tab key. The command line parser will complete the command if the string entered is unique to the command. Another option will be to type the first few letters followed by? This will show all the commands that start with the letters you had already typed.

## 1.2. Command History

Use the Up/Down arrows keys to scroll between the commands you had already typed. To display the entire history **#show history** command can be used



## 2. GENERAL MAINTENANCE COMMANDS

### 2.1. configure terminal

Description – Start unit configuration. Terminal display will switch from # to **(config)#**

**configure terminal**

Parameter	parameter	description
Parameter	-	N.A
Default	N.A	
Mode	EXEC	
Usage	Enter configuration mode whenever starting unit configuration	
Example	# configure terminal. <b>NOTE</b> - You may also use the shortcut # conf t	

### 2.2. interface

Description – Start interface (port) configuration. Terminal display will switch from **(config)#** to **(config-if)#**

**interface** <port\_type> [ <port\_type\_list> ]

**NOTE:**

It is possible to configure same parameter for multiple interface by using syntax as 1/1-8 (configure same value for ports 1-8) as described in the command example

Parameter	parameter	description
Parameter	<port_type>	Port type GigabitEthernet, vlan
	[ <port_type_list> ]	List of Port ID, ex. 1/1,3-5 1/1-8 1/1,2,4
Default	N.A	
Mode	Global Configuration	
Usage	Enter interface configuration mode to start configuring port parameters	
Example	<b>Example#1 (enter configuration mode for ports 1, 3,4 and 5):</b> (config)# interface GigabitEthernet 1/1,3-5 (config-if)# <b>Example#2 (enter configuration mode for ports 1 through 8)</b> (config)# interface GigabitEthernet 1/1-8 (config-if)#	

### 2.3. exit

Description - Go up one level in the configuration process. Logout from terminal/telnet/SSH session in case user was at top level.

#### exit

Parameter	parameter	description
Parameter	-	N.A
Default	N.A	
Mode	Exit from current mode	
Usage	Whenever end in-depth configuration and need to go up one level, or to log out of the serial interface.	
Example	<b>Example#1:</b> (config)# exit # <b>Example#2:</b> (config-if)# exit (config)#	

### 2.4. end

Description - End any in-depth configuration mode and go back to EXEC mode

#### end

Parameter	parameter	description
Parameter	-	N.A
Default	N.A	
Mode	Go back to EXEC mode	
Usage	Whenever need to end in-depth configuration and go back to EXEC mode	
Example	<b>Example#1:</b> (config-if)# end # <b>Example#2:</b> (config)# end #	

## 2.5. show running-config

Description - View unit running configuration (the configuration being in use by the unit). User may change unit configuration without saving the changes, meaning that upon unit power down-up cycle it may operate completely different.

### show running-config

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to view the current configuration	
Example	# show running-config	

## 2.6. show running-config all-default

Description - View unit running configuration plus omitted default configuration

### show running-config all-default

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to view the current configuration including all default values	
Example	# show running-config all-default	

## 2.7. dir

Description - Show all optional configuration files stored inside the unit.

### dir

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to view all configuration files stored in the flash.	
Example	# dir	

## 2.8. copy running-config startup-config

Description– update (save) unit configuration to be used after reset or power-up.

### copy running-config startup-config

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to save unit configuration	
Example	# copy running-config startup-config	

## 2.9. copy running-config flash:<file-name>

Description- copy running (or startup) configuration files to another file name or to TFTP server. Also vice versa from TFTP Server to unit local file

**copy** <running config | startup-config | flash:file-name | tftp://server/filename>

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to copy unit configuration to another file or to TFTP Server or from TFTP Server to unit local file	
Example	<p><b>Example#1 - save current configuration stored in unit flash to another file named "test" also inside unit FLASH.</b></p> <pre># copy running-config flash:test</pre> <p><b>Example#2 - save unit running configuration file to TFTP Server under name "test"</b></p> <pre># copy running-config tftp://192.168.0.40/test</pre>	

## 2.10. del flash:<file-name>

Description - delete configuration file stored in flash

**del** flash:<file-name>

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to delete unit configuration stored in flash	
Example	# del flash:test	

## 2.11. reload cold

Description – Unit performs software reset, turning Ethernet ports down and back up.

### reload cold

#### NOTE:

Unit software reset may or may-not effect PoE power being delivered to PD devices.

Use the command “`poe uninterruptible-power`”, “`no poe uninterruptible-power`” to configure PoE power state during software reset cycle.

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to restart the unit	
Example	# reload cold	

## 2.12. reload defaults

Description – restore to full factory default configuration

### reload defaults

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to restore to factory default	
Example	# reload defaults	

## 2.13. reload defaults keep-ip

Description - Semi factory defaults, keeping IP and VLAN configuration unchanged

### reload defaults keep-ip

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to restore to factory default but keep IP address unchanged.	
Example	# reload defaults keep-ip	

## 2.14. show version

Description – Display unit software and hardware information

### show version

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to display unit information	
Example	<pre># show version Software Version : 1.13 (created on 2019-01-30T18:29:03+02:00) PoE Firmware    : 24034356.1056.003 MAC Address     : 00-05-5a-98-67-23 Serial Number   : 000038 Production Number : 8301 System Date &amp; Time : 1970-01-13T20:20:55+00:00 System Uptime   : 12d 20:20:55</pre>	

### 3. NETWORK

#### 3.1. Ethernet ports - configuration commands

Configure Ethernet ports Link speed, max Ethernet packet size and flow control

##### 3.1.1. Shutdown

Description- Enable/disable Ethernet port (has no effect on PoE power).

**shutdown**

**no shutdown**

Parameter	parameter	description
Parameter	-	-
Default	N.A	
Mode	Port List Interface configuration mode	
Usage	Use the command to disable the specified interface and use no form of this command to enable the interface	
Example	<p><b>Example#1 (disable port 1)</b>  # configure terminal  (config)# interface GigabitEthernet 1/1  (config-if)# shutdown</p> <p><b>Example#2 (disable ports 1 through 8)</b>  # configure terminal  (config)# interface GigabitEthernet 1/1-8  (config-if)# shutdown</p> <p><b>Example#3 (enable all ports)</b>  # configure terminal  (config)# interface *  (config-if)# no shutdown</p>	

### 3.1.2. Speed

Description- configure port speed.

**speed** { 1000 | 100 | 10 | auto }

Parameter	parameter	description
	10	10Mbps
	100	100Mbps
	1000	1000Mbps (1Gbps)
	auto	Auto negotiation
Default	All ports are set to Auto	
Mode	Port List Interface Mode	
Usage	Use to set the speed of the specified interface	
Example	<p><b>Example#1 (set speed for port 1 to 100Mbps)</b></p> <pre># configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# speed 100</pre> <p><b>Example#2 (set all ports to 1Gbps)</b></p> <pre># configure terminal (config)# interface * (config-if)# speed 1000</pre>	



### 3.1.3. Duplex

Description- configure interface duplex mode

**duplex** { half | full | auto }

**no duplex**

Parameter	parameter	description
	half	Forced half duplex
	full	Forced full duplex
	auto	Auto negotiation of duplex mode.
Default	All ports are set to Auto	
Mode	Port List Interface Mode	
Usage	Use to set the duplex mode of the specified interface. Use the no form of the command to set duplex to default	
Example	<p><b>Example#1 (set duplex for port 1 to half)</b></p> <pre># configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# duplex half</pre> <p><b>Example#2 (set all ports to 1Gbps)</b></p> <pre># configure terminal (config)# interface * (config-if)# speed 1000</pre>	

### 3.1.4. flowcontrol

Description- configures flow control for the interface (slow temporarily packet transition upon request, or for packet reception, signal the remote transmitter to slow down temporarily its packet transition whenever Switch reception buffer becomes to full).

**flowcontrol** { on | off }

**no flowcontrol**

Parameter	parameter	description
	on	Enable flow control.
	off	Disable flow control.
Default	All ports flow control receive and send is off.	
Mode	Port List Interface Mode	
Usage	Use to set the flow control for the interface. Use the no form of the command to return to defaults.	
Example	<p><b>Example#1 (enable flow control for port 1)</b>            # configure terminal            (config)# interface GigabitEthernet 1/1            (config-if)# flowcontrol on</p> <p><b>Example#2 (enable flow control for all ports)</b>            # configure terminal            (config)# interface *            (config-if)# flowcontrol on</p>	

### 3.1.5. MTU

Description- specify maximum Ethernet frame size for the interface

**mtu** <max\_length>

**no mtu**

Parameter	parameter	description
	<max_length>	Maximum frame size in bytes (1518-9600 bytes)
Default	All ports mtu 9600 bytes	
Mode	Port List Interface Mode	
Usage	Use to set the maximum frame size for the interface. Use the no form of the command to return to defaults.	
Example	<p><b>Example#1 (set mtu for port 1 to 1518)</b>            # configure terminal            (config)# interface GigabitEthernet 1/1            (config-if)# mtu 1518</p> <p><b>Example#2 ( set mtu for all ports to 1518)</b>            # configure terminal            (config)# interface *            (config-if)# mtu 1518</p>	

## 3.2. Ethernet ports - view commands

View link status (up/down/speed), flow control, max frame size and mode.

### 3.2.1. Show interface status

Description- display status and configuration information for any port.

**show interface** <port\_type> [ <v\_port\_type\_list> ] **status**

Parameter	parameter	description
	<port_type>	Port type in GigabitEthernet
	<v_port_type_list>	List of Port ID, ex, 1/1,3-5;2/2-4,6
Default	N.A	
Mode	EXEC mode	
Usage	Use to display current status of the specified interface	
Example	<p><b>Example#1 (show status and configuration for port#1)</b>  # show interface GigabitEthernet 1/1 status</p> <p><b>Example#2 (show status and configuration for ports #1 through #5)</b>  # show interface GigabitEthernet 1/1-5 status</p> <pre># show interface GigabitEthernet 1/1-5 status Interface          Mode      Speed &amp; Duplex  Flow Control  Max Frame  Excessive  Link ----- GigabitEthernet 1/1  enabled  Auto           disabled      9600       Discard    100fdx GigabitEthernet 1/2  enabled  Auto           disabled      9600       Discard    Down GigabitEthernet 1/3  enabled  Auto           disabled      9600       Discard    Down GigabitEthernet 1/4  enabled  Auto           disabled      9600       Discard    Down GigabitEthernet 1/5  enabled  Auto           disabled      9600       Discard    Down #</pre>	

### 3.3. IPv4, IPv6 – configuration commands

Configure static/dynamic IPv4, IPv6 address and mask, default gateway, DNS.

#### 3.3.1. ip name-server - DNS Server

Description- Set the DNS server for resolving domain names

```
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> ] }
```

```
no ip name-server
```

Parameter	parameter	description
	<order>	Preference of DNS server. Default selection is 0
	<v_ipv4_ucast>	A valid IPv4 unicast address
	<v_ipv6_ucast>	A valid IPv6 unicast address
	dhcp	Dynamic Host Configuration Protocol
Default	No DNS server configured	
Mode	Global Configuration mode	
Usage	Set the DNS for resolving domain names. Use the no version of the command to return to default.	
Example	<p><b>Example#1 ( DNS Server 0 setting is derived from any DHCPv4 VLANs-ID)</b>            (config)# ip name-server 0 dhcp</p> <p><b>Example#2 ( DNS Server 1 configured as a static IPv4 address)</b>            (config)# ip name-server 1 192.168.0.10</p> <p><b>Example#3 (DNS Server 1 setting is derived from DHCPv4 VLANs-ID 1)</b>            (config)#ip name-server 1 dhcp ipv4 interface vlan 1</p>	

### 3.3.2. ip (ipv6) address - IPv4,IPv6 interface

Description- add IPv4, IPv6 interface

```
ip address { { <address> <netmask> } | { dhcp [ fallback <fallback_address> <fallback_netmask>
[ timeout <fallback_timeout> ] ] [ client-id { <port_type> <client_id_interface> | ascii <ascii_str> | hex
<hex_str> } ] [ hostname <hostname> ] ] }
```

**no ip address**

**ipv6 address** <subnet>

**no ipv6 address**

Parameter	parameter	description
Parameter	<address>	IPv4 address
	<netmask>	IP netmask
	dhcp	Enable Dynamic Host Configuration Protocol
	fallback	DHCP fallback settings
	client-id	DHCP client identifier
	hostname	DHCP host name
	<subnet>	IPv6 prefix x:x::y/z
Default	N.A	
Mode	VLAN Interface Configuration mode	
Usage	Add VLAN interface and set all IPv4, IPv6 parameters. Use the no version of the command to disable the selected VLAN interface. To remove it completely use <b>no interface vlan &lt;id&gt;</b> from Global configuration mode.	
Example	<p><b>Example#1 ( Set VLAN2 static IP address to 192.168.1.50 mask length 24)</b>  (config)#interface vlan 2  (config-if-vlan)# ip address 192.168.1.50 255.255.255.0</p> <p><b>Example#2 ( Add VLAN 3 and set it to get IP address from DHCP using MAC of port 1 as Client ID with a hostname test)</b>  (config)#interface vlan 3  (config-if-vlan)# ip address dhcp client-id GigabitEthernet 1/1 hostname test</p>	

### 3.3.3. IP Routes (Default gateway)

Description- Add new IP route.

**ip route** <ipv4\_addr> <ipv4\_netmask> <ipv4\_gw> [ <distance> ]

**no ip route** <ipv4\_addr> <ipv4\_netmask> <ipv4\_gw>

Parameter	parameter	description
	<ipv4_addr>	Network
	<ipv4_netmask>	Netmask
	<ipv4_gw>	Gateway
	<distance>	Distance value for this route
Default	N.A	
Mode	Global Configuration mode	
Usage	To route all unknown destination IP to default gateway use the following parameters: Network=0.0.0.0 Netmask=0.0.0.0 and Distance=1 To remove the route use <b>no ip route</b> command with all parameters for the selected route.	
Example	<b>Example#1 (add IP route to gateway 192.168.1.1)</b> (config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1 1 <b>Example#2 (remove IP route)</b> (config)#no ip route 0.0.0.0 0.0.0.0 192.168.1.1	

### 3.4. IPv4, IPv6 – view commands

#### 3.4.1. Show interface vlan

Description - View VLAN interface status and configuration

**show interface vlan** [ <vlist> ]

Parameter	parameter	description
	<vlist>	vlan list
Default	N.A	
Mode	EXEC mode	
Usage	Use to display current status and configuration of the specified interface	
Example	<b>Example#1 (show status and configuration for VLAN 1)</b> <pre># show interface vlan 1 # show interface vlan 1 VLAN1   LINK: 00-05-5a-98-67-23 Mtu:1500 &lt;UP BROADCAST MULTICAST&gt;   IPV4: 192.168.0.50/24 192.168.0.255   IPV6: fe80::205:5aff:fe98:6723/64 &lt;&gt;</pre>	

### 3.5. NTP (Network Time Protocol) – configuration commands

Configure the unit NTP Servers IP. The NTP Server updates the unit with the correct GMT (Greenwich Mean Time).

#### 3.5.1. ntp server - Configure NTP server

Description- Enable or disable NTP server and specify its parameters. Up to 5 NTP servers can be configured.

**ntp**

**no ntp**

**ntp server** <index\_var> ip-address { <ipv4\_var> | <ipv6\_var> | <name\_var> }

**no ntp server** <index\_var>

Parameter	parameter	description
	<index_var>	NTP Server index (1-5)
	<ipv4_var>	IPv4 address of NTP server
	<ipv6_var>	IPv6 address of NTP server
	<name_var>	Domain name of NTP server
Default	N.A	
Mode	Global Configuration mode	
Usage	Enable NTP server by entering ntp command. Use a no version of the command to disable it. Specify the parameters of NTP server by entering ntp server command. Use a no version of the command to delete the specified NTP server.	
Example	<p><b>Example#1 (add NTP server 1 with IP address 192.168.1.2)</b>            (config)#ntp server 1 ip-address 192.168.1.2</p> <p><b>Example#2 ( add NTP server 2 with domain name ntp.microsemi.com)</b>            (config)#ntp server 2 ip-address ntp.microsemi.com</p> <p><b>Example#3 (enable NTP server)</b>            (config)#ntp</p>	

### 3.6. NTP (Network Time Protocol) – view commands

#### 3.6.1. show ntp status - view NTP status

Description - View NTP status and all configured NTP servers

**show ntp status**

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC mode	
Usage	Use the command view status and configuration of NTP servers	
Example	<p><b>Example#1</b>            #show ntp status</p>	

### 3.7. Time Zone – configuration commands

Configure unit local time zone and daylight saving.

#### 3.7.1. clock timezone - time zone configuration

Description - configure time zone.

**clock timezone** <word16> <hour\_var> [ <minute\_var> [ <subtype\_var> ] ]

**no clock timezone**

Parameter	parameter	description
	<word16>	Name of time zone up to 16 characters. Use “ for null input
	< hour_var >	Hours offset from UTC -23-23
	<minute_var>	Minutes offset from UTC 0-59
	<subtype_var>	Sub type of time zone 0-9
Default	(UTC) Coordinated Universal Time	
Mode	Global Configuration mode	
Usage	Specify the time zone and offsets from UTC. Use the no form of the command to return to default	
Example	<b>Example#1 (Configure Eastern time zone with -05:00 from UTC)</b> (config)#clock timezone Eastern -05 0	



### 3.8. clock summer-time - Daylight Savings Time configuration

Description - Configure daylight savings time.

**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>  
]]

**no clock summer-time**

Parameter	parameter	description
	<word16>	Name of time zone in summer up to 16 characters. Use “ for null input
	<start_month_var>	Month to start (1-12)
	<start_date_var>	Date to start (1-31)
	<start_year_var>	Year to start (2000-2097)
	<start_hour_var>	Time to start (hh:mm)
	<end_month_var>	Month to end (1-12)
	<end_date_var>	Date to end (1-31)
	<end_year_var>	Year to end (2000-2097)
	<end_hour_var>	Time to end (hh:mm)
	<offset_var>	Offset to add in minutes (1-1439)
	<start_week_var>	Week number to start (1-5)
	<start_day_var>	Weekday to start (1-7)
	<end_week_var>	Week number to end (1-5)
	<end_day_var>	Weekday to end (1-7)
Default	Daylight savings time mode disabled	
Mode	Global Configuration mode	
Usage	Configure summer (daylight savings) time in absolute non-recurring mode ( <b>date</b> ) and recurring mode ( <b>recurring</b> ). Use the no form of the command to go back to default.	
Example	<b>Example#1 (Configure non-recurring Daylight Savings Time to start on March 10 2019 at 02:00AM and finish on November 3 2019 at 02:00AM)</b> (config)#clock summer-time " date 3 10 2019 02:00 11 3 2019 02:00	

### 3.9. Time zone - view commands

#### 3.9.1. show clock detail

Description - Display the detailed clock information

##### show clock detail

	parameter	description
Parameter	N.A	N.A
Default	N.A	
Mode	EXEC mode	
Usage	Use to display clock information	
Example	<b>Example</b> # show clock detail	

### 3.10. SysLog report – configuration commands

Configure SysLog Server IP address. The unit sends SysLog messages during Power-Up and normal operation. The SysLog events are send by the unit over the Network to SysLog Server. The user has the option to filter some of the SysLog messages being send by the unit by configuring from what severity/importance SysLog messages the message should be send.

#### 3.10.1. logging - Enable and configure SysLog

Description - System Log configuration commands

##### logging on

**logging host** { <ipv4\_addr> | <domain\_name> }

**logging level** { informational | notice | warning | error }

##### no logging on

	parameter	description
Parameter	<ipv4_addr>	Name of time zone up to 16 characters. Use “ ” for null input
	<domain_name>	Hours offset from UTC -23-23
	informational	Severity 6: Informational messages
	notice	Severity 5: Normal but significant condition
	warning	Severity 4: Warning conditions
	error	Severity 3: Error conditions
Default	N.A	
Mode	Global Configuration mode	
Usage	Enable SysLog server, specify its address and what level of messages will be sent to it. Use the no logging on command to disable SysLog server.	
Example	<b>Example#1 (Enable SysLog server at 192.168.0.1 with Warning level messages)</b> (config)#logging on (config)#logging host 192.168.0.1 (config)#logging level warning <b>Example#2 (Disable SysLog server)</b> (config)#no logging on	

### 3.11. SysLog report – view commands

#### 3.11.1. show logging

Description - Show logging configuration and message summary.

**show logging** [ informational ] [ notice ] [ warning ] [ error ]

**show logging** <log\_id> [ switch <switch\_list> ]

Parameter	parameter	description
	informational	Severity 6: Informational messages
	notice	Severity 5: Normal but significant condition
	warning	Severity 4: Warning conditions
	error	Severity 3: Error conditions
	<log_id>	Message logging ID
	<switch_list>	List of switch ID (in a stacked system) ex, 1,3-5,7
Default	N.A	
Mode	EXEC mode	
Usage	Display SysLog server status and configuration and detailed logging messages.	
Example	<b>Example#1 (Show SysLog configuration on switch 1 and detailed log message 1)</b> #show logging 1 switch 1 <b>Example#2 ( Show SysLog configuration and detailed Error log messages)</b> #show logging error	

### 3.12. MAC Table Learning – configuration commands

Provides various options regarding the way MAC address learning should be processed by the Ethernet Switch, and how to process a packet with unknown source MAC address, unknown destination MAC address, etc.

When a packet is received, it is classified by its Source-MAC, Destination-MAC, VLAN-ID and Port number. As part of Ethernet Switch forwarding algorithm, the switch will look for Destination-MAC and VLAN inside the MAC learning table. If it was found, then the packet will be forwarded to the specified port, otherwise the packet is flooded to all ports on same VLAN.

### 3.12.1. mac address-table aging-time

Description- By default, dynamic entries are removed from the Mac table after 300 seconds. This process is called aging. Aging time can be configured to be in the range of 10 to 1000000 seconds or 0 to disable automatic aging.

**mac address-table aging-time** <v\_0\_10\_to\_1000000>

**no mac address-table aging-time**

Parameter	parameter	description
Parameter	<v_0_10_to_1000000>	Aging time in seconds, 0 disables aging
Default	Aging time is 300 seconds	
Mode	Global Configuration mode	
Usage	Set MAC address table aging time in seconds. Use the no version of the command to reset to default (300 seconds)	
Example	<b>Example#1 (Set aging time to 400 seconds)</b> (config)# mac address-table aging-time 400 <b>Example#2 ( Disable automatic aging)</b> (config)# mac address-table aging-time 0	

### 3.12.2. mac address-table learning

Description - Each port can do learning in Auto mode (done automatically as soon as the frame with unknown MAC is received) or Secured mode (only static MAC entries are learned and all other frames are dropped). MAC learning can also be disabled and no learning is done. Specific VLANs can also be learning-disabled.

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

**no mac address-table learning**

**mac address-table learning vlan** <vlan\_list>

**no mac address-table learning vlan** <vlan\_list>

Parameter	parameter	description
Parameter	[ secure ]	Port Secure mode
Default	All ports are in Auto learning mode	
Mode	Port List Interface Mode (for specific port), Global Configuration Mode (for VLANs)	
Usage	Set MAC address table learning mode to Secure or back to Auto ( command without [ secure ] parameter). Use the no version of the command to Disable learning.	
Example	<b>Example#1 (Set MAC address learning to Secure on port 1)</b> (config)# interface GigabitEthernet 1/1 (config-if)#mac address-table learning secure <b>Example#2 ( Disable MAC address learning on ports 2-5)</b> (config)# interface GigabitEthernet 1/2-5 (config-if)#no mac address-table learning <b>Example#3 (add VLAN2 to the list of learning disabled VLANs)</b> (config)# no mac address-table learning vlan 2	

### 3.12.3. mac address-table static

Description - Assign a static mac address to the specific port or ports

```
mac address-table static <v_mac_addr> vlan <v_vlan_id> { [ interface <port_type>
[ <v_port_type_list> ] ] }
```

```
no mac address-table static <v_mac_addr> vlan <v_vlan_id> { [ interface <port_type>
[ <v_port_type_list> ] ] }
```

Parameter	parameter	description
	<v_mac_addr>	48 bit MAC address: xx:xx:xx:xx:xx:xx
	<v_vlan_id>	VLAN IDs 1-4095
	<port_type>	GigabitEthernet
	<v_port_type_list>	List of Port ID, ex, 1/1,3-5
Default	N.A	
Mode	Global Configuration Mode	
Usage	Assigns a static MAC address to a port. Use the no version of the command to remove it.	
Example	<b>Example#1 (Assign static MAC address 00:11:22:33:44:55 to port 1 on VLAN 1)</b> (config)#mac address-table static 00:11:22:33:44:55 vlan 1 interface Gi 1/1	

### 3.13. MAC Table Learning – view commands

#### 3.13.1. show mac address-table

Description - Display MAC address table entries.

**show mac address-table** [ conf | static | aging-time | { { learning | count } [ interface <port\_type> [ <v\_port\_type\_list> ] | vlan <v\_vlan\_id\_2> ] } | { address <v\_mac\_addr> [ vlan <v\_vlan\_id> ] } | vlan <v\_vlan\_id\_1> | interface <port\_type> [ <v\_port\_type\_list\_1> ] ]

Parameter	parameter	description
Parameter	conf	User added static MAC addresses
	static	All static MAC addresses
	aging-time	Display MAC address aging time
	learning	MAC address learning state (Learn/Secure/Disable)
	count	Total number of MAC addresses
Default	N.A	
Mode	EXEC Mode	
Usage	Show MAC address table entries in various views based on the specific parameter.	
Example	<p><b>Example#1 (display all static MAC addresses)</b>  #show mac address-table static</p> <p><b>Example#2 (display the MAC table entry for MAC address 00:11:22:33:44:55)</b>  #show mac address-table address 00:11:22:33:44:55</p> <p><b>Example#3 (display the MAC table entry for port 2)</b>  #show mac address-table interface GigabitEthernet 1/2</p> <p><b>Example#4 (display all MAC table entries)</b>  #show mac address-table</p> <pre># show mac address-table Type   VID  MAC Address          Ports Static 1    00:00:00:00:00:11   GigabitEthernet 1/3-5 Dynamic 1    00:05:5a:03:99:b6   GigabitEthernet 1/9 Static 1    00:05:5a:98:67:23   CPU Dynamic 1    00:0a:cd:2d:b1:ed   GigabitEthernet 1/10 Dynamic 1    18:68:cb:b5:85:03   GigabitEthernet 1/1 Static 1    33:33:00:00:00:01   GigabitEthernet 1/1-11 CPU Static 1    33:33:ff:98:67:23   GigabitEthernet 1/1-11 CPU Static 1    ff:ff:ff:ff:ff:ff   GigabitEthernet 1/1-11 CPU</pre>	

### 3.14. Routing – view commands

#### 3.14.1. show ip route

Description- Display IPv4 route entry table with status information.

##### show ip route

Parameter	parameter	description
Parameter	N.A	N.A
Default	N.A	
Mode	EXEC Mode	
Usage	display routing information	
Example	<p><b>Example</b></p> <pre>#show ip route # show ip route Codes: C - connected, S - static, O - OSPF,       * - selected route, D - DHCP installed route  C* 192.168.0.0/24 is directly connected, VLAN 1 #</pre>	

## 4. ACCESS CONTROL

Control who can access the unit, from what type of Network interface, who will verify remote user username and password (by the unit locally, or by RADIUS/TACACS+ Authentication Server), etc.

### 4.1. Local Users - configuration commands

Allows changing 'admin' user password, adding or removing additional users and changing users' password.

#### 4.1.1. username -Add local user or change password

Description- Add, remove or change password of local users. Up to 20 users can be configured.

**username** { default-administrator | <input\_username> } **privilege** <priv> **password** { unencrypted <unency\_password> | encrypted <ency\_password> | none }

**no username** <username>

Parameter	parameter	description
	<input_username>	User name allows letters, numbers and underscores
	<priv>	User privilege level 0-15. <b>NOTE - Please use only privilege level 15</b>
	<unency_password>	The UNENCRYPTED (Plain Text) user password. Any printable characters including space are accepted. Notice that you have no chance to get the Plain Text password after this command. The system will always display the ENCRYPTED password.
	<ency_password>	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.
	none	NULL password
Default	N.A	
Mode	Global Configuration Mode	
Usage	Add a new user for the local switch access and add/change password.	
Example	<b>Example#1 (add a user named usertest with unencrypted password of testuser)</b> (config)# username usertest privilege 15 password unencrypted testuser <b>Example#2 (remove user named usertest)</b> (config)# no username usertest <b>Example#3 (change the password of usertest to testuser123 )</b> (config)# username usertest privilege 15 password unencrypted testuser123	

#### NOTE:

**NOTE-1:** The unit is shipped with default username 'admin' and with no password. It is strongly recommended to assign a strong password instead.

**NOTE-2:** Username 'admin' can't be removed or be changed, only its password.



## 4.2. Local Users - view commands

### 4.2.1. show user-privilege

Description- Display all local users, privilege levels and passwords

#### show user-privilege

Parameter	parameter	description
Parameter	N.A	N.A
Default	N.A	
Mode	EXEC Mode	
Usage	display information about all local user accounts	
Example	<b>Example</b> <pre># show user-privilege # show user-privilege username admin privilege 15 password encrypted 64d0dfc93d6b24b6ad00! 0dc81cb0e9865f737d4d7d1fb8e83be6cb687dd5fce85a26d9d21a754b753d1a1</pre>	

### 4.2.2. show users ← New command, need to update TOC

Description- Display information on how remote users are connected at the moment to the unit. Serial is represented as “con”, Telnet is represented as “vty”.

#### show users

Parameter	parameter	description
Parameter	N.A	N.A
Default	N.A	
Mode	EXEC Mode	
Usage	Display information on how remote users are connected	
Example	<b>Example</b> <pre># show users # show users Line is con 0. * You are at this line now. Connection is from Console. User name is admin. Privilege is 15. Elapsed time is 0 day 0 hour 12 min 48 sec. Idle time is 0 day 0 hour 0 min 0 sec.  Line is vty 0. Connection is from 192.168.0.40:63043 by Telnet. User name is admin. Privilege is 15. Elapsed time is 0 day 0 hour 5 min 29 sec. Idle time is 0 day 0 hour 5 min 29 sec.</pre>	

## 4.3. Web Server - configuration commands

Controls whether unit embedded Web Server should operate in HTTP or HTTPS mode. HTTPS use TLS v1.2 encryption to encrypt all Web Network traffic between the user web browser and the unit Web Server.

### 4.3.1. ip http secure-server

Description- Configure Web Server to use only HTTPS (secure and encrypted operation mode) or HTTP (unsecure operation mode) as well.

**ip http secure-server**

**no ip http secure-server**

	parameter	description
Parameter	N.A	N.A
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure Web Server to use HTTPS. Use the no version of the command to use HTTP	
Example	<b>Example</b> (config)# ip http secure-server (config)# no ip http secure-server	

### 4.3.2. ip http secure-certificate

Description- Manage Web Server certificate. Use this command to delete the current certificate, generate a new self-signed RSA certificate or upload a PEM certificate using URL over http, tftp or ftp.

**ip http secure-certificate** { upload <url\_file> [ pass-phrase <pass\_phrase> ] | delete | generate }

	parameter	description
Parameter	<url_file>	Uniform Resource Locator. It is a specific character string that constitutes a reference to a resource. Syntax: <protocol>://[<username>[:<password>]@]<host>[:<port>]/<path>]/<file_name> If the following special characters: space !"#\$%&'()*+,-./:;<=>?@[\\]^_{ }~ need to be contained in the input URL string, they should be percent-encoded. 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.
	<pass_phrase>	Privacy key pass phrase string if uploading certificate protected by a specific passphrase.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Manage the HTTPS certificate (PEM format)	
Example	<b>Example#1 (upload the HTTPS certificate from TFTP server)</b> (config)# ip http secure-certificate upload tftp://10.9.52.103/test_ca.pem <b>Example#2 (delete current certificate)</b> (config)# ip http secure-certificate delete	

## 4.4. Web Server - view commands

### 4.4.1. show ip http

Description- Use this command to show status information about the secure HTTP web server.

#### show ip http

	parameter	description
Parameter	N.A	N.A
Default	N.A	
Mode	EXEC Mode	
Usage	Display the secure HTTP web server status	
Example	<b>Example</b> <pre># show ip http Switch secure HTTP web server is enabled Switch secure HTTP web redirection is enabled Switch secure HTTP certificate is presented</pre>	

## 4.5. Telnet/SSH/Web - configuration commands

**Authentication Method Configuration** - Configures Which Network interface as telnet, SSH, Web or local console should be enabled or disable, and how remote user username + password will be authenticated. Should it be done locally by the unit or by remote RADIUS/TACACS+ Authentication Server.

**Accounting Method Configuration** - Configures if the unit should send Accounting messages to remote TACACS+ Accounting server whenever remote user login/logout, and report any CLI command typed by the user over Console, Telnet or SSH.

### 4.5.1. aaa authentication login

Description- Configure how a user is authenticated when logging into the switch via one of the management client interfaces - console, telnet, ssh or web. Each one of the interfaces may have up to 3 authentication servers. In case the first authentication server is down, then second authentication server will be accessed instead. Same for the third authentication server in case both the first and second authentication servers are down.

**NOTE:**



**NOTE1 – Rejection of remote user by any of the authentication servers will reject the remote user. The three remote authentication servers are used only as a backup in case one of the authentication services is down.**

**NOTE – disabling authentication by all three authentication services will disable management interface ( console, Telnet, SSH, Web)**

Local- use the Switch local user database.

radius- use remote RADIUS server

tacacs- use remote TACACS+ server.

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

**no aaa authentication login** { console | telnet | ssh | http }

	parameter	description
Parameter	N.A	N.A
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure user authentication method for a specific management interface. Use the no version of the command to disable the interface.	
Example	<p><b>Example#1 (configure SSH to be authenticated 1st by RADIUS Server. In case it is down, then by TACACS Server, and in case it is also down, then be authenticated locally)</b></p> <pre>(config)#aaa authentication login ssh radius tacacs local (config)# aaa authentication login ssh radius tacacs local</pre> <p><b>Example#2 (disable Telnet remote access)</b></p> <pre>(config)# no aaa authentication login telnet</pre>	

#### 4.5.2. aaa accounting

Description - Configure what type of activity over a specific interface (console, telnet or ssh) is reported to the TACACS+ accounting server. Possible options are “CLI Commands”, and Exec=Login/Logout. CLI Commands - every CLI command entered by the user will be mirrored to the accounting server. Exe (Login/Logout) – every login/logout of remote user will be reported to the accounting server.

**aaa accounting** { console | telnet | ssh } tacacs { [ commands <priv\_lvl> ] [ exec ] }

**no aaa accounting** { console | telnet | ssh }

Parameter	parameter	description
	[commands <priv_lvl> ]	all CLI commands equal and above the privilege level are accounted
	[ exec ]	only remote user login/logout is reported
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure accounting method and reporting. Use the no version of the command to disable accounting.	
Example	<p><b>Example#1 (configure accounting for ssh to report all CLI activity and any login/logout )</b>            (config)# aaa accounting ssh tacacs commands 15 exec</p> <p><b>Example#1 (disable accounting for Telnet)</b>            (config)# no aaa accounting telnet</p>	

## 4.6. Telnet/SSH/Web - view commands

### 4.6.1. show aaa

Description - Display the current authentication, authorization and accounting statuses and methods for all interfaces.

#### show aaa

Parameter	parameter	description
Parameter	N.A	N.A
Default	N.A	
Mode	EXEC Mode	
Usage	Display the current status of authentication, authorization and accounting.	
Example	<p><b>Example</b></p> <pre># show aaa # show aaa Authentication :   console : local   telnet  : disable   ssh    : radius tacacs local   web    : local Authorization :   console : no, commands disabled   telnet  : no, commands disabled   ssh    : no, commands disabled Accounting :   console : no, commands disabled, exec disabled   telnet  : no, commands disabled, exec disabled   ssh    : tacacs, commands 15 enabled, exec enabled</pre>	

## 4.7. Access Control List - configuration commands

Access Control List - configures from what remote IP address remote user will be able to access the Switch management interface over Web, SNMP, Telnet/SSH.

### 4.7.1. access management

Description - Enable/disable access management mode and configure up to 16 entries.

**access management**

**no access management**

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

**no access management** <access\_id\_list>

Parameter	parameter	description
	<access_id>	ID of access management entry (1-16)
	<access_vid>	VLAN ID for the access management entry (1-4095)
	<start_addr>	start IPv4 or IPv6 unicast address
	<end_addr>	end IPv4 or IPv6 unicast address
Default	N.A	
Mode	Global Configuration Mode	
Usage	Enable access management mode and configure up to 16 entries. Use the no version of the command to disable access management globally or a specific entry.	
Example	<p><b>Example#1 (configure access management entry 1 on VLAN4 for IPv4 address 192.168.0.40 – 192.168.0.70 on all interfaces)</b>            (config)# access management 1 4 192.168.0.40 to 192.168.0.70 all</p> <p><b>Example#1 (disable access management entry 1)</b>            (config)# no access management 1</p>	

## 4.8. Access Control List - view commands

### 4.8.1. show access management

**show access management** [ statistics | <access\_id\_list> ]

Parameter	parameter	description
Parameter	<access_id_list>	ID of access management entry (1~16)
Default	N.A	
Mode	EXEC Mode	
Usage	Display access management status and all entries or statistics or a specific entry.	
Example	<p><b>Example#1 (show access management configuration)</b></p> <pre># show access management Switch access management mode is disabled W: WEB/HTTPS S: SNMP T: TELNET/SSH  Idx VID  Start IP Address          End IP Address          W S T ----- 1   4    192.168.0.40              192.168.0.70          Y Y Y</pre> <p><b>Example#2 (show access management statistics)</b></p> <pre>#show access management statistics  # show access management statistics Access Management Statistics: ----- HTTP   Receive:    0   Allow:      0   Discard:    0 HTTPS  Receive:    0   Allow:      0   Discard:    0 SNMP   Receive:    0   Allow:      0   Discard:    0 TELNET Receive:    0   Allow:      0   Discard:    0 SSH    Receive:    0   Allow:      0   Discard:    0</pre>	



## 5. VLAN

### 5.1. VLAN configuration commands and port types

**VLAN Access** - VLAN is a mean to split Switch ports into sub port groups while each group is totally isolated from the other as if we are using two or more independent Switches. Such splitting is done by assigning different VLAN-IDs to various groups of ports, each group is assigned a different VLAN-ID and the ports for each group are configured as Access ports meaning that VLAN tagging and port splitting is done internally by the switch. The packets transmitted over Access ports are the normal Ethernet ports with no VLAN tagging.

**VLAN Trunk** – VLAN Trunk port configuration allow multiple VLAN-IDs to travel over the same Ethernet cable or local LAN Network with absolute isolation between the VLANs traveling over the same infrastructure

#### **VLAN port types:**

Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.

#### **VLAN port type - Unaware:**

On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.

#### **VLAN port type - C-Port:**

On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag.

If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.

#### **VLAN port type - S-Port:**

On egress, if frames must be tagged, they will be tagged with an S-tag.

On ingress, frames with a VLAN tag with TPID = 0x88A8 get classified to the VLAN ID embedded in the tag.

Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped.

#### **NOTE:**

 If the S-port is configured to accept Tagged and Untagged frames (see [Ingress Acceptance](#) below), frames with a C-tag are treated like frames with an S-tag.


If the S-port is configured to accept Untagged Only frames, S-tagged frames will be discarded (except for priority S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID.

**VLAN port type - S-Custom-Port:**

On egress, if frames must be tagged, they will be tagged with the custom S-tag.

On ingress, frames with a VLAN tag with a TPID equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped.

**NOTE:**

 If the custom S-port is configured to accept Tagged and Untagged frames (see [Ingress Acceptance below](#)), frames with a C-tag are treated like frames with a custom S-tag.

If the Custom S-port is configured to accept Untagged Only frames, custom S-tagged frames will be discarded (except for priority custom S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID

**5.1.1. vlan - create VLAN**

Description- Create one or more VLANs in **Access mode**. By default, only single VLAN #1 is enabled with all ports assigned to this VLAN in Access mode..

**vlan** <vlist>

**no vlan** <vlist>

Parameter	parameter	description
	<vlist>	ISL VLAN IDs. Individual elements are separated by commas and ranges are specified with a dash.
Default	None	
Mode	Global Configuration mode	
Usage	Create allowed Access VLANs. Use the no version of the command to delete VLANs.	
Example	<b>Example#1 (Create Access VLANs 10,11,12,200 and 300)</b> (config)# vlan 10-12,200,300 <b>Example#2 ( Delete VLAN 12)</b> (config)# no vlan 12	

### 5.1.2. vlan ethertype s-custom-port

Description- Specifies the EtherType/TPID (specified in hexadecimal) used for Custom S-Ports. The setting is in force for all ports set to S-Custom port type.

#### NOTE:

S-Custom VLAN port type is used whenever double VLAN tagging (Q-in-Q, 802.1ad) is in use.



**vlan ethertype s-custom-port** <etype>

Parameter	parameter	description
Parameter	<etype>	EtherType (Range: 0x0600-0xffff)
Default	TPID is set to 0x88A8	
Mode	Global Configuration mode	
Usage	Specifies the ethertype/TPID for Custom S-Ports	
Example	<b>Example#1 (Set TPID=8888)</b> (config)# vlan ethertype s-custom-port 0x8888 <b>Example#2 ( Set TPID back to default 88A8)</b> (config)# no vlan ethertype s-custom-port	

### 5.1.3. switchport mode

Description- Defines the port mode as access (default), trunk or hybrid unconditionally.

**switchport mode** { access | trunk | hybrid }

Parameter	parameter	description
Parameter	access	Configure a switch port mode is access
	trunk	Configure a switch port mode is trunk
	hybrid	Configure a switch port mode is hybrid
Default	The switch port default mode is access	
Mode	Port List Interface Mode	
Usage	Set port mode	
Example	<b>Example#1 (configure the port 3 mode as trunk)</b> # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode trunk	

#### 5.1.4. switchport trunk native vlan

Description - Configure VLAN ID to be added internally by the Switch whenever native VLAN packet (packet with no VLAN header) is received.

**switchport trunk native vlan** <pvid>

**no switchport trunk native vlan**

Parameter	parameter	description
		<pvid>
Default	Trunk native default VLAN is VLAN1	
Mode	Port List Interface Mode	
Usage	Configure a port VLAN ID for a trunk port. use the no version of the command to revert to default.	
Example	<b>Example#1 (configure port 3 as trunk with PVID 4)</b> # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode trunk (config-if)# switchport trunk native vlan 4	

#### 5.1.5. switchport trunk vlan tag native

Description- Port in Trunk mode may control the tagging of frames on egress. Options are default Untag Port VLAN (frames classified to the Port VLAN are transmitted untagged and all other frames are transmitted with the relevant tag) and Tag all (all frames transmitted with a tag).

**switchport trunk vlan tag native**

**no switchport trunk vlan tag native**

Parameter	parameter	description
		N.A
Default	Frames classified to the Port VLAN (Native VLAN) do not get tagged on egress.	
Mode	Port List Interface Mode	
Usage	Set the trunk port egress tagging to all. Use the no version of the command to revert to default (untag native VLAN)	
Example	<b>Example#1 (configure port 3 as trunk with PVID 4 and set egress tagging to tag all)</b> # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode trunk (config-if)# switchport trunk native vlan 4 (config-if)# switchport trunk vlan tag native	

### 5.1.6. switchport trunk allowed vlan

Description- Ports in Trunk mode may control which VLANs they are allowed to become members of. By default, Trunk port will become a member of all VLANs (1-4095).

**switchport trunk allowed vlan** { all | none | [ add | remove | except ] <vlan\_list> }

**no switchport trunk allowed vlan**

Parameter	parameter	description
	all	all VLANs are allowed (1-4095)
	none	Port will not become member of any VLAN
	add	Add VLANs to the current list
	remove	Remove VLANs from the current list
	except	All VLANs except the following (VLAN ID or list)
	<vlan_list>	VLAN IDs of the allowed VLANs. Individual elements are separated by commas and ranges are specified with a dash.
Default	All VLANs are allowed (1-4095)	
Mode	Port List Interface Mode	
Usage	Configure allowed VLANs for a trunk port. Use the no version of the command to revert to default.	
Example	<b>Example#1 (configure port 3 as trunk and exclude VLAN 10 and 30,31,32 from allowed VLANs)</b> # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan except 10,30-32	

### 5.1.7. switchport forbidden vlan

Description- Configure the port to never become a member of one or more VLANs.

**switchport forbidden vlan** { add | remove } <vlan\_list>

**no switchport forbidden vlan**

Parameter	parameter	description
	add	Add forbidden VLANs to the current list of forbidden VLANs
	remove	Remove forbidden VLANs from the current list of forbidden VLANs
Default	Trunk Port may become a member of all possible VLANs	
Mode	Port List Interface Mode	
Usage	Configure VLANs that a trunk port may not become a member. Use the no version of the command to revert to default.	
Example	<b>Example#1 (configure port 3 as trunk and add VLAN 4 to the list of forbidden VLANs)</b> # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode trunk (config-if)# switchport forbidden vlan add 4	

### 5.1.8. switchport hybrid native vlan

Description - Configure VLAN ID (PVID) for the hybrid port (Native VLAN).

**switchport hybrid native vlan** <pvid>

**no switchport hybrid native vlan**

Parameter	parameter	description
	<pvid>	VLAN ID of the native VLAN when this port is in hybrid mode
Default	Hybrid native default VLAN is VLAN1	
Mode	Port List Interface Mode	
Usage	Configure a port VLAN ID for a hybrid port. Use the no version of the command to revert to default	
Example	<b>Example#1 (configure port 4 as hybrid with PVID 5)</b> # configure terminal (config)# interface GigabitEthernet 1/4 (config-if)# switchport mode hybrid (config-if)# switchport hybrid native vlan 5	

### 5.1.9. switchport hybrid port-type

Description- Specifies the port type in hybrid mode.

**switchport hybrid port-type** { unaware | c-port | s-port | s-custom-port }

**no switchport hybrid port-type**

Parameter	parameter	description
	unaware	Port is not aware of VLAN tags. No matter the received frame is tagged or untagged, port adds a tag (based on PVID) to the frame and then forward it.
	c-port	Customer port. If the received frame is untagged, C-port adds a tag (based on PVID) to the frame and then forward it; If the frame is already tagged, it will be forwarded without adding a tag.
	s-port	Provider port. Port only accepts untagged frames. If the received frame is untagged, S-port adds a tag (based on PVID) to the frame and then forward it; If the frame is already tagged, it will be discarded.
	s-custom-port	Custom provider port. When Ethertype is set to 0x8100, S-custom ports do the same as C-ports: If the received frame is untagged, S-custom port adds a tag (based on PVID) to the frame and then forward it; If the frame is already tagged, it will be forwarded without adding a tag.
Default	Hybrid Port type is C-port	
Mode	Port List Interface Mode	
Usage	Configure hybrid port type. Use the no version of the command to revert to default.	
Example	<b>Example#1 (configure port 3 as hybrid Unaware type)</b> # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode hybrid (config-if)# switchport hybrid port-type unaware	

### 5.1.10. switchport hybrid ingress-filtering

Description- enable/disable ingress filtering

**switchport hybrid ingress-filtering**

**no switchport hybrid ingress-filtering**

Parameter	parameter	description
		N.A
Default	Ingress filtering disabled	
Mode	Port List Interface Mode	
Usage	Enable ingress filtering Use the no version of the command to revert to default.	
Example	<b>Example#1 (configure port 3 as hybrid and enable ingress filtering)</b> # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode hybrid (config-if)# switchport hybrid ingress-filtering	

### 5.1.11. switchport hybrid acceptable-frame-type

Description- Set Ingress acceptance criteria.

**switchport hybrid acceptable-frame-type { all | tagged | untagged }**

**no switchport hybrid acceptable-frame-type**

Parameter	parameter	description
	all	Both tagged and untagged frames are accepted
	tagged	Only frames tagged with the corresponding port type tag are accepted.
	untagged	Only untagged frames are accepted.
Default	Hybrid Port is set to accept all frames (tagged and untagged)	
Mode	Port List Interface Mode	
Usage	Configure type of frames accepted on ingress. use the no version of the command to revert to default.	
Example	<b>Example#1 (configure port 3 as hybrid and accept tagged frames only on ingress)</b> # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode hybrid (config-if)# switchport hybrid acceptable-frame-type tagged	



### 5.1.12. switchport hybrid egress-tag

Description- Configure Egress tagging.

**switchport hybrid egress-tag** { none | all [ except-native ] }

**no switchport hybrid egress-tag**

Parameter	parameter	description
	none	No Egress tagging. All frames transmitted without a tag.
	all	Tag all frames. All frames are transmitted with a tag.
	except-native	Tag all frames except frames classified to native VLAN.
Default	Hybrid Port is set to tag all frames except frames classified to native VLAN.	
Mode	Port List Interface Mode	
Usage	Configure egress tagging. Use the no version of the command to revert to default.	
Example	<b>Example#1 (configure port 3 as hybrid and set egress tagging to all)</b> # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode hybrid (config-if)# switchport hybrid egress-tag all	

### 5.1.13. switchport trunk allowed vlan

Description- Ports in Hybrid mode may control which VLANs they are allowed to become members of. By default Hybrid port will become a member of all VLANs (1-4095).

**switchport hybrid allowed vlan** { all | none | [ add | remove | except ] <vlan\_list> }

**no switchport hybrid allowed vlan**

Parameter	parameter	description
	all	all VLANs are allowed (1-4095)
	none	Port will not become member of any VLAN
	add	Add VLANs to the current list
	remove	Remove VLANs from the current list
	except	All VLANs except the following (VLAN ID or list)
	<vlan_list>	VLAN IDs of the allowed VLANs. Individual elements are separated by commas and ranges are specified with a dash.
Default	All VLANs are allowed (1-4095)	
Mode	Port List Interface Mode	
Usage	Configure allowed VLANs for a hybrid port. Use the no version of the command to revert to default.	
Example	<b>Example#1 (configure port 3 as hybrid and exclude VLAN 10 and 30,31,32 from allowed VLANs)</b> # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode hybrid (config-if)# switchport hybrid allowed vlan except 10,30-32	

## 5.2. View VLAN Members

### 5.2.1. show vlan

Description- provides overview of membership status of VLAN users and VLANs configured for each interface.

**show vlan** [ id <vlan\_list> | name <name> | brief ] [ all ]

Parameter	parameter	description
	id <vlan_list>	VLAN status by VLAN ID
	name <name>	VLAN status by VLAN name
	brief	VLAN summary informatin
	all	Show all VLANs (if left out only access VLANs are shown)
Default	N.A	
Mode	EXEC mode	
Usage	Display VLAN membership status overview.	
Example	<b>Example#1 (Show VLAN summary information for all vlans)</b> #show vlan brief all <b>Example#2 ( Show VLAN information for port 1 configured by Admin)</b> #show vlan status interface GigabitEthernet 1/1 admin	

## 5.3. View VLAN Ports

### 5.3.1. show vlan status

Description- Shows VLAN status for a specific interface (port) configured by a specific user.

**show vlan status** [ interface <port\_type> [ <plist> ] ] [ admin | all | combined | conflicts | mstp | nas | rmirror ]

Parameter	parameter	description
	interface <port_type>	Show the VLANs configured for a specific interface or interfaces and port type (GigabitEthernet)
	<plist>	List of Port ID, ex, 1/1,3-5
	admin	Show the VLANs configured by administrator.
	all	Show VLANs configured VLANs for all VLAN users.
	combined	Show the combined set of configured VLANs.
	mstp	Show the VLANs configured by MSTP.
	nas	Show the VLANs configured by NAS.
	rmirror	Show the VLANs configured by Remote mirroring.
Default	N.A	
Mode	EXEC mode	
Usage	Display VLAN membership status overview.	
Example	<b>Example#1 ( Show VLAN information for port 1 configured by Admin)</b> #show vlan status interface GigabitEthernet 1/1 admin	

## 6. POE-BT POWER

### 6.1. PoE-BT Power configuration commands

PoE-BT (IEEE 802.3-bt) is the latest PoE (Power Over Ethernet) specification offering up to 90[W] of power whenever power is delivered over all four RJ45 cable pairs.

#### 6.1.1. poe extended-bt-power-mode

Description- Global configuration of Extended Power Mode. When enabled the switch will extend slightly the maximum power provided to PD beyond its classification. For example, class 8 will be extended from 90W to 95W.

**poe extended-bt-power-mode**

**no poe extended-bt-power-mode**

	parameter	description
Parameter	N.A	N.A
Default	Extended mode disabled.	
Mode	Global Configuration Mode	
Usage	Enable extended power mode. Use the no version of the command to disable extended power mode.	
Example	<b>Example</b> (config)# poe extended-bt-power-mode	

#### 6.1.2. poe uninterruptible-power

Description - Global configuration of uninterruptible power mode. When enabled, the switch will provide seamless uninterruptible power to PD devices even when the switch performs software reset.

**poe uninterruptible-power**

**no poe uninterruptible-power**

	parameter	description
Parameter	N.A	N.A
Default	Uninterruptible power enabled	
Mode	Global Configuration Mode	
Usage	Enable uninterruptible power mode. Use the no version of the command to disable uninterruptible power mode.	
Example	<b>Example</b> (config)# poe uninterruptible-power	

**6.1.3. poe power**

Description- Enable/Disable poe power for the specific port

**poe power**

**no poe power**

Parameter	parameter	description
Parameter	N.A	N.A
Default	N.A	
Mode	Port List Interface Mode	
Usage	Enable/Disable PoE power for the port.	
Example	<b>Example#1 (enable PoE power for port 1)</b> (config)# interface GigabitEthernet1/1 (config-if)# poe power <b>Example#2 (disable PoE power for port 2)</b> (config)# interface GigabitEthernet1/2 (config-if)# no poe power	

**6.1.4. poe mode**

Description - Set PoE mode to control what PD devices may receive power.

**poe mode { bt | bt-plus-legacy }**

Parameter	parameter	description
Parameter	bt	Power only PoE-BT compliant PDs.
	bt-plus-legacy	Power PoE-BT compliant and legacy PDs.
Default	N.A	
Mode	Port List Interface Mode	
Usage	Set PoE mode	
Example	<b>Example#1 (set PoE mode for port 1 to BT only)</b> (config)# interface GigabitEthernet1/1 (config-if)# poe mode bt	

**6.1.5. poe priority**

Description- Configure PoE priority

**poe priority** { low | high | critical }

Parameter	parameter	description
Parameter	low	Low priority. Ports will be powered last upon startup and disconnected first whenever power budget is exceeded.
	high	High priority. Ports will be powered second upon startup and disconnected second whenever power budget is exceeded.
	critical	Critical priority. Ports will be powered first upon startup and disconnected last whenever power budget is exceeded.
Default	All ports priority is Low.	
Mode	Port List Interface Mode	
Usage	Set PoE priority	
Example	<b>Example#1 (set PoE priority for port 1 to high)</b> (config)# interface GigabitEthernet1/1 (config-if)# poe priority high	

**6.1.6. poe terminal-description**

Description- Textual description for each PoE-PD device connected to the port.

**poe terminal-description** <term\_desc>

Parameter	parameter	description
Parameter	<term_desc>	PD device description (32 characters).
Default	N.A	
Mode	Port List Interface Mode	
Usage	Set terminal description	
Example	<b>Example#1 (set description for port 1 to ipcamera)</b> (config)# interface GigabitEthernet1/1 (config-if)# poe terminal description "ipcamera"	

## 6.2. PoE-BT Power view commands

### 6.2.1. show poe

Description- Display detailed PoE status for the switch.

**show poe** [ interface <port\_type> [ <v\_port\_type\_list> ] ]

Parameter	parameter	description
	interface <port_type>	Specify interfaces and port type (GigabitEthernet)
	<v_port_type_list>	List of Port ID, ex, 1/1,3-5
Default	N.A	
Mode	EXEC Mode	
Usage	Display PoE status for the switch.	
Example	<p><b>Example#1 (show poe status for port 1)</b>  # show poe interface GigabitEthernet 1/1</p> <p><b>Example#2 (show poe status for all ports)</b>  # show poe</p> <pre># show poe ----- Interface          PD Class  Power Alloc [w]  Port Status  Power Used [w]  Current Used [mA]  Internal status ----- GigabitEthernet 1/1  2         7             PoE-ON (2Pair)  2.7           50                0x85 PoE-On : 4P Pwr on 2P IEEE SSPD GigabitEthernet 1/2  ---        0             ---           0              0                 0xA8 PoE-Off: No Device (open) GigabitEthernet 1/3  4, 4      60           PoE-ON         2.8           53                0x89 PoE-On : 4P Pwr on 4P IEEE DSPD GigabitEthernet 1/4  ---        0             ---           0              0                 0xA8 PoE-Off: No Device (open) GigabitEthernet 1/5  ---        0             PoE-OFF-fault  0             0                 0x41 PoE-Off: PD Class &gt; PoE-IC max Class GigabitEthernet 1/6  ---        0             PoE-OFF-fault  0             0                 0x25 PoE-Off: PD Capacitor out of range GigabitEthernet 1/7  ---        0             ---           0              0                 0xA8 PoE-Off: No Device (open) GigabitEthernet 1/8  ---        0             ---           0              0                 0xA8 PoE-Off: No Device (open) ----- .. Total              67              5.5           103</pre>	

## 7. SPANNING TREE

### 7.1. STP Bridge Configuration commands

Spanning Tree Protocol (STP), and its variations as RSTP and MSTP, is used to prevent possible Network loops which without STP will cause broadcast storming. It also offers redundancy path from Switch to Switch or path to path over multiple Switches by supporting Network loops under the control of STP. STP algorithm will make sure that at any given time only one path out of multiple possible loops will be active, those allowing the Switch to use multiple backup paths in case main connection path go down.

#### 7.1.1. spanning-tree mode

Description- Configure STP protocol version.

**spanning-tree mode** { stp | rstp | mstp }

**no spanning-tree mode**

Parameter	parameter	description
	stp	Spaning Tree protocol 802.1D
	rstp	Rapid Spanning Tree protocol 802.1w
	mstp	Multiple Spanning Tree protocol 802.1s
Default	Default protocol is MSTP	
Mode	Global Configuration Mode	
Usage	Set STP protocol version. Use the no version of the command to revert to default.	
Example	<b>Example#1 (set STP to RSTP)</b> # configure terminal (config)# spanning-tree mode rstp	

#### 7.1.2. spanning-tree system settings

Description- Configure STP system settings used by all STP Bridge instances in the switch.

Basic STP global setting commands:

**spanning-tree mst** <instance=0> **priority** <prio>

**spanning-tree mst hello-time** <hellotime>

**spanning-tree mst forward-time** <fwdtime>

**spanning-tree mst max-age** <maxage> [ forward-time <fwdtime> ]

**spanning-tree mst max-hops** <maxhops>

**spanning-tree transmit hold-count** <holdcount>

Advanced STP global setting commands:

**spanning-tree edge bpdu-filter**

**spanning-tree edge bpdu-guard**

**spanning-tree recovery interval** <interval>



Parameter	parameter	description
	<instance>	STP bridge instance. Must be 0 (zero)
	priority <prio>	Bridge Priority. Supported values are 0-61440. Only values divisible by 4096 are allowed. For example, 4096, 8192, etc. . Default value is 32768
	<hellotime>	Interval between sending STP BPDUs. Valid values are 1-10 seconds. Default is 2 seconds.
	<fwdtime>	Forward delay used by STP Bridges to transit Root and Designated Ports to Forwarding. Valid values are 4-30 seconds. Default is 15.
	<maxage>	Maximum age of the information transmitted by the Bridge when it is a Root Bridge. Valid values are 6-40 seconds. Default is 20.
	<maxhops>	Defines how many bridges a root bridge can distribute its BPDU information. Valid values are 6-40 hops. Default is 20.
	<holdcount>	Number of BPDUs a bridge port can send per second. Valid range 1-10 BPDUs per second. Default is 6.
	<interval>	Time to pass before a port in error-disabled state can be enabled. Values are 30-86400 seconds (24 hours). Default is port error recovery disabled.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure STP system settings. Use the no version of the command to revert to default.	
Example	<b>Example (Configure STP settings)</b> <pre># configure terminal (config)# spanning-tree mode mstp (config)# spanning-tree mst 0 priority 36864 (config)# spanning-tree mst hello-time 3 (config)# spanning-tree mst max-age 25 forward-time 16 (config)# spanning-tree mst max-hops 25 (config)# spanning-tree transmit hold-count 7 (config)# spanning-tree edge bpdu-filter (config)# spanning-tree edge bpdu-guard (config)# spanning-tree recovery interval 120</pre>	

### 7.1.3. spanning-tree port settings

Description- Configure STP CIST settings for the specific physical and aggregated ports

**spanning-tree** *Enable STP on the port*

**no spanning-tree** *Disable STP on the port*

**spanning-tree mst** <instance=0> **cost** { <cost> | auto }

**spanning-tree mst** <instance=0> **port-priority** <prio>

**spanning-tree edge**

**spanning-tree auto-edge**

**spanning-tree restricted-role**

**spanning-tree restricted-tcn**

**spanning-tree bpduguard**

**spanning-tree link-type** { point-to-point | shared | auto }

Parameter	parameter	description
	<instance>	STP bridge instance. Must be 0 (zero)
	<b>cost</b> { <cost>   auto }	Controls the path cost incurred by the port. Auto setting will set the cost as appropriate by link speed using 802.1D recommended values. User defined value can also be entered and the valid range is 1-200000000. Default is auto.
	<b>port-priority</b> <prio>	Represents the port priority. Must be divisible by 16, supported values are 0-240. For example, 16, 32, etc. Default value is 128
	<b>link-type</b> { point-to-point   shared   auto }	Controls whether the port connects to a point-to-point LAN rather than to a shared medium. Default is auto.
	<b>edge</b>	Defines whether the port is connecting directly to edge devices. Default is non-edge.
	<b>auto-edge</b>	Enables auto edge detection on the port.
	<b>restricted-role</b>	If enabled causes the port not to be selected as Root port.
	<b>restricted-tcn</b>	If enabled causes the port not to propagate received topology change notifications to other ports.
	<b>bpduguard</b>	If enabled causes the port to disable itself upon receiving valid BPDUs.
Default	N.A	
Mode	Port List Interface Mode	
Usage	Configure STP CIST settings for the specific physical and aggregated ports. Use the no version of the command to revert to default.	
Example	<p><b>Example (Configure STP CIST settings for port 1)</b></p> <pre># configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# spanning-tree (config-if)# spanning-tree mst 0 cost auto (config-if)# spanning-tree mst 0 port-priority 16 (config-if)# spanning-tree edge</pre>	

```
(config-if)# spanning-tree restricted-role
(config-if)# spanning-tree bpduguard
(config-if)# spanning-tree link-type point-to-point
```

## 7.2. STP Bridges view commands

### 7.2.1. show spanning-tree

Description- Provides a detailed status information on a STP bridge instance, along with port state for all active ports associated.

**show spanning-tree** [ summary | active | { interface <port\_type> [ <v\_port\_type\_list> ] } | { detailed [ interface <port\_type> [ <v\_port\_type\_list\_1> ] ] } | { mst [ configuration | { <instance> [ interface <port\_type> [ <v\_port\_type\_list\_2> ] ] } ] } ] }

Parameter	parameter	description
	summary	STP summary
	active	STP active interfaces
	interface <port_type>	Choose port and type in GigabitEthernet
	<v_port_type_list>	List of Port ID, ex, 1/1,3-5
	detailed	STP statistics
	mst	Multiple STP
	configuration	Show MSTI to VLAN mapping
	<instance>	STP bridge instance (CIST=0, MSTI1=1...)
Default	N.A	
Mode	EXEC Mode	
Usage	Display information on STP	
Example	<p><b>Example (Display CIST port state for port 8)</b>  # show spanning-tree interface GigabitEthernet 1/8</p> <p><b>Example (Display STP detailed Bridge status)</b>  #show spanning-tree mst 0</p>	

## 8. SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

Application-layer protocol used to manage and monitor network devices and their functions. It enables network management systems to learn network problems by receiving traps or change notices from network devices.



### NOTE:

By default, SNMP is disabled for security concerns. In case SNMPv2 will be used then please change SNMPv2 default 'public', 'private' community strings (passwords) prior enabling SNMPv2.

### 8.1. Enable/Disable SNMP and configure MIB-II system OIDs

#### 8.1.1. snmp-server

Description- Enable/Disable SNMP server

**snmp-server**

**no snmp-server**

	parameter	description
Parameter	N.A	N.A
Default	N.A	
Mode	Global Configuration Mode	
Usage	Enable SNMP server. Use the no version of the command to disable SNMP.	
Example	<b>Example (Enable SNMP)</b> # configure terminal (config)# snmp-server	

### 8.1.2. snmp-server contact, System-Name (host) and location

Description- Specify SNMP MIB-II contact person, system name and system location

**snmp-server contact** <v\_line255>

**no snmp-server contact**

**host** <conf\_name>

**snmp-server location** <v\_line255>

Parameter	parameter	description
	<v_line255>	String length is 0-255 and valid ASCII characters range 32-126
	<conf_name>	Administratively assigned name for this system. By convention this is fully-qualified domain name. String length is 0-255 and no spaces are permitted.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Specify system contact, name and location Use the no version of the command to delete it.	
Example	<p><b>Example (Set system contact as “testcontact”, name as “microchip” and location as “server room”)</b></p> <pre># configure terminal (config)# snmp-server contact testcontact (config)# host microchip microchip(config)# snmp-server location server room</pre>	

## 8.2. SNMPv2-v3 Configuration commands

### 8.2.1. snmp-server view

Description- Configure which SNMP OIDs should be included/excluded from the entire SNMP OID tree.

**snmp-server view** <view\_name> <.oid\_subtree> { include | exclude }

**no snmp-server view** <view\_name> <oid\_subtree>

Parameter	parameter	description
Parameter	<view_name>	Name identifying the view OID branch to be included/excluded. String length is 1-32 and valid ASCII characters range 33-126
	<.oid_subtree>	OID defining the root of the subtree to add to the named view. String length is 1-128. Allowed string content is number or asterisk (*).
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure SNMP View OID-range.	
Example	<p><b>Example (Create SNMP view OID-range named “mib-ii” with access to all SNMP OIDs except for MIB-II system branch .1.3.6.1.2.1.1)</b></p> <pre># configure terminal (config)# snmp-server view mib-ii .1.3.6.1.2.1.1 excluded</pre>	

### 8.2.2. snmp-server community

Description- Configure SNMP community table used as part of SNMP group configuration.

**snmp-server community** <comm> [ { ip-range <v\_ipv4\_addr> <v\_ipv4\_netmask> } ] { <sec> | encrypted <sec\_enc> }

Parameter	parameter	description
Parameter	<comm>	Community Name to map to the SNMP Groups configuration. String length is 1-32 and valid ASCII characters range 33-126.
	ip-range <v_ipv4_addr> <v_ipv4_netmask>	Indicates SNMP access source address. A range of source addresses can be used to restrict source subnet when combined with source netmask.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure SNMP community	
Example	<p><b>Example (Create SNMP community named “c-name” with community secret “secret”)</b></p> <pre># configure terminal (config)# snmp-server community c-name secret</pre>	

### 8.2.3. snmp-server user

Description - Configure SNMPv3 user.

**snmp-server user** <username> engine-id <engineID> [ { md5 { <md5\_passwd> | { encrypted <md5\_passwd\_encrypt> } } | sha { <sha\_passwd> | { encrypted <sha\_passwd\_encrypt> } } } [ priv { des | aes } { <priv\_passwd> | { encrypted <priv\_passwd\_encrypt> } } ] ]

Parameter	parameter	description
Parameter	<username>	User name. String length is 1-32 and valid ASCII characters range 33-126
	<engineID>	Octet string. Must contain an even number (in hexadecimal format) between 10 and 64 digits.
	md5 <md5_passwd>	Authentication protocol MD5 and password length 8-32 ASCII characters 33-126
	sha <sha_passwd>	Authentication protocol SHA and password length 8-40 ASCII characters 33-126
	priv { des   aes }	Privacy protocol DES or AES
	<priv_passwd>	Privacy password length 8-32 ASCII characters 33-126.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure SNMPv3 user.	
Example	<b>Example (Add SNMPv3 user testuser with authentication protocol MD5 and password testpassword)</b> # configure terminal (config)# snmp-server user testuser engine-id 800019ab12345 md5 testpassword	

### 8.2.4. snmp-server security-to-group model

Description- Configure SNMP group-name based on Security Model and Security name.

**snmp-server security-to-group model** { v1 | v2c | v3 } name <security\_name> group <group\_name>

Parameter	parameter	description
Parameter	v1   v2c   v3	Security model the entry should belong to.
	<security_name>	One of the security names created in SNMP Community for v1 and v2c or one of the SNMPv3 users.
	<group_name>	Group name. String length is 1-32 and valid ASCII characters range 33-126.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure SNMP group name.	
Example	<b>Example (Configure SNMPv2 security model and group)</b> # configure terminal (config)# snmp-server security-to-group model v2c name public group ro_group	

### 8.2.5. snmp-server access

Description- Configure SNMP access.

**snmp-server access** <group\_name> model { v1 | v2c | v3 | any } level { auth | noauth | priv } [ read <view\_name>] [ write <write\_name>]

Parameter	parameter	description
	<group_name>	Group name previously configured by security-to-group command. String length is 1-32 and valid ASCII characters range 33-126.
	model {v1   v2c   v3   any}	Security model the entry should belong to.
	level {auth   noauth   priv}	Security level. authNoPriv, noAuthNoPriv, authPriv
	read <view_name>	Name of the MIB view defining the MIB objects for which this request may read OID values
	write <write_name>]	Name of the MIB view defining the MIB objects for which this request may set OID new values
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure SNMP group name.	
Example	<b>Example (Configure SNMPv2 access)</b> # configure terminal (config)# snmp-server access ro_group model v2c level noauth read mib-ii	

### 8.2.6. snmp-server trap

Description- SNMP Trap source configuration. Provides the list for all events that may cause SNMP Trap to be sent.

**snmp-server trap** <source\_name>

**no snmp-server trap** <source\_name>

Parameter	parameter	description
	<source_name>	Name of the event. Possible options are: coldStart, warmStart, linkUp, linkDown, authenticationFailure, newRoot, topologyChange, lldpRemTablesChange.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure SNMP source. Use the no version of the command to delete the entry.	
Example	<b>Example (Add “Remote SNMP client was trying to access the unit using invalid username/password values” event to the trap source configuration)</b> # configure terminal (config)# snmp-server trap authenticationfailure	



### 8.2.7. snmp-server host

Description- Add/delete SNMP trap server.

**snmp-server host** <conf\_name>

**no snmp-server host** <conf\_name>

**host** { <v\_ipv4\_ucast> | <v\_word> } [ <udp\_port> ] [ traps | informs ]

Parameter	parameter	description
Parameter	<conf_name>	Group name previously configured by security-to-group command. String length is 1-32 and valid ASCII characters range 33-126.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Add SNMP trap server. Use the no version of the command to delete trap server.	
Example	<b>Example (Add SNMP Trap server “trapserver”)</b> # configure terminal (config)# snmp-server host trapserver	

Configure SNMP Trap server

**version** { v1 [ { <v1\_comm> | encrypted <v1\_comm\_sec> } ] | v2 [ { <v2\_comm> | encrypted <v2\_comm\_sec> } ] | v3 engineID <v\_word10\_to\_64> [ <securityname> ] }

**host** { <v\_ipv4\_ucast> | <v\_word> } [ <udp\_port> ] [ traps | informs ]

**informs retries** <retries> timeout <timeout>

Parameter	parameter	description
Parameter	<v1_comm>, <v2_comm>, <v_word10_to_64>	SNMP version 1 and 2 community or version 3 engine ID
	<v_ipv4_ucast>	IP address of SNMP trap host
	<v_word>	hostname of SNMP trap host
	<udp_port>	UDP port of the trap messages
	traps	Send Trap messages to this host
	informs	Send Inform messages to this host
	<retries>	inform retry times 0-255
	<timeout>	inform timeout interval 0-2147 seconds
Default	N.A	
Mode	SNMP Server Host Mode	
Usage	Configure SNMP trap server.	
Example	<b>Example (Configure SNMP Trap server)</b> # configure terminal (config)# snmp-server host trapserver (config-snmp-host)# version v2 c-name (config-snmp-host)# host my.traphost.com 162 informs (config-snmp-host)# informs retries 6 timeout 3	

### 8.3. SNMP view commands

#### 8.3.1. show snmp

Description- Display SNMP configuration.

**show snmp view** - Display Oid-range configuration

**show snmp community** -Display SNMP Community configuration

**show snmp security-to-group** -Display SNMP Group configuration

**show snmp access** - Display SNMP access configuration

**show snmp user** - Display SNMPv3 users

**show snmp trap** - Display configured SNMP Trap sources

**show snmp host** - Display SNMP Trap server list and configuration

	parameter	description
Parameter	N.A	N.A
Default	N.A	
Mode	EXEC Mode	
Usage	Display PoE status for the switch.	
Example	<b>Example (Display SNMP Trap server list and configuration)</b> # show snmp host	

## 9. RADIUS TACACS+

### 9.1. RADIUS Server configuration commands

RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access Control System) are networking protocols that provide centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect to the unit over Web, telnet, SSH. Remote username and password is send to RADIUS/TACACS+ Server for authentication (user + password match/don't match) and Authorization (privilege level) rather being tested locally using unit local configuration file.

#### 9.1.1. Global configuration commands

Description- Set default values to be used for every new RADIUS server being added when the same parameters are left blank.

**radius-server timeout** <seconds>

**radius-server retransmit** <retries>

**radius-server deadtime** <minutes>

**radius-server key** { [ unencrypted ] <unencrypted\_key> | encrypted <encrypted\_key> }

Parameter	parameter	description
	<b>timeout</b> <seconds>	Time to wait for a RADIUS server to reply in seconds 1-1000 before retransmitting the request
	<b>retransmit</b> <retries>	Number of times 1-1000 a request is retransmitted to a server that is not responding.
	<b>deadtime</b> <minutes>	Period between 0-1440 minutes during which the switch will not send a new request to a server that failed to respond to previous requests (dead).
	<b>key</b>	Specify the encryption key up to 63 characters long.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure default global parameters for RADIUS Server	
Example	<b>Example</b> # configure terminal (config)# radius-server timeout 10 (config)# radius-server retransmit 3 (config)# radius-server deadtime 10 (config)# radius-server key unencrypted secret	

### 9.1.2. Radius server configuration

Description - Add a new RADIUS server. Up to 5 servers can be added.

```
radius-server host <host_name> [ auth-port <auth_port> ] [ acct-port <acct_port> ] [ timeout
<seconds> ] [ retransmit <retries> ] [ key { [ unencrypted ] <unencrypted_key> | encrypted
<encrypted_key> } ]
```

Parameter	parameter	description
Parameter	<host_name>	IPv4/IPv6 address or the hostname of the radius server
	<auth_port>	UDP port number to use on the RADIUS server for authentication. Set to 0 to disable authentication.
	<acct_port>	UDP port number to use on the RADIUS server for accounting. Set to 0 to disable accounting.
	timeout <seconds>	Time to wait for this RADIUS server to reply (overrides default).
	retransmit <retries>	Specify the number of retries to active server (overrides default).
	<unencrypted_key>	The UNENCRYPTED (Plain Text) secret key (overrides default)
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure custom parameters for RADIUS Server.	
Example	<b>Example</b> # configure terminal (config)# radius-server host radiusserver auth-port 1812 timeout 20 retransmit 5	

## 9.2. RADIUS Server Status view commands

### 9.2.1. show radius-server

Description - Display overview status of the current RADIUS servers configuration and statistics

```
show radius-server [ statistics ]
```

Parameter	parameter	description
Parameter	[ statistics ]	provides detailed statistics for the RADIUS servers
Default	N.A	
Mode	EXEC Mode	
Usage	Show current RADIUS servers configuration and statistics	
Example	<b>Example#1 (Display RADIUS server status)</b> # show radius-server <b>Example#2 (Display Radius server status and statistics)</b> # show radius-server statistics	

### 9.3. TACACS+ Server configuration commands

#### 9.3.1. Global configuration commands

Description- Set default values to be used for every new TACACS+ server being added when the same parameters are left blank.

**tacacs-server timeout** <seconds>

**tacacs-server deadtime** <minutes>

**tacacs-server key** { [ unencrypted ] <unencrypted\_key> | encrypted <encrypted\_key> }

Parameter	parameter	description
	<b>timeout</b> <seconds>	Time to wait for a TACACS+ server to reply in seconds 1-1000 before retransmitting the request
	<b>deadtime</b> <minutes>	Period between 0-1440 minutes during which the switch will not send a new request to a server that failed to respond to previous requests (dead).
	<b>key</b>	Specify the encryption key up to 63 characters long.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure default global parameters for TACACS Server	
Example	<p><b>Example</b></p> <pre># configure terminal (config)# tacacs-server timeout 10 (config)# tacacs-server deadtime 3 (config)# tacacs-server key unencrypted secret</pre>	

### 9.3.2. TACACS+ Server configuration

Description - Add a new TACACS+ server. Up to 5 servers can be added.

**tacacs-server host** <host\_name> [ port <port> ] [ timeout <seconds> ] [ key { [ unencrypted ] <unencrypted\_key> | encrypted <encrypted\_key> } ]

Parameter	parameter	description
	<host_name>	IPv4/IPv6 address or the hostname of the radius server
	<port>	TCP port number to use on the TACACS+ server for authentication.
	timeout <seconds>	Time to wait for this TACACS+ server to reply (overrides default).
	<unencrypted_key>	The UNENCRYPTED (Plain Text) secret key (overrides default)
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure custom parameters for TACACS+ Server.	
Example	<b>Example</b> # configure terminal (config)# tacacs-server host tacacsserver port 50 timeout 20 key unencrypted secret	

### 9.4. TACACS+ Server view commands

#### 9.4.1. show tacacs-server

Description - Display current TACCAS+ servers configuration.

**show tacacs-server**

Parameter	parameter	description
	N.A	
Default	N.A	
Mode	EXEC Mode	
Usage	View the current TACACS+ server configuration.	
Example	<b>Example#1 (Display TACACS+ server configuration)</b> # show tacacs-server	

## 10. AGGREGATION/LACP

### 10.1. Aggregation Group Configuration commands

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

#### 10.1.1. aggregation mode

Description - Specify parameters that contribute to the way Aggregation is done. Applies to the whole network element.

**aggregation mode** { [ smac ] [ dmac ] [ ip ] [ port ] }

**no aggregation mode**

Parameter	parameter	description
	[ smac ]	Source MAC address can be used to calculate the destination port for the frame (enabled by default)
	[ dmac ]	Destination MAC address can be used to calculate the destination port for the frame (disabled by default)
	[ ip ]	IP address can be used to calculate the destination port for the frame (enabled by default)
	[ port ]	TCP/UDP port number can be used to calculate the destination port for the frame (enabled by default)
Default	smac,ip and port enabled, dmac disabled	
Mode	Global Configuration Mode	
Usage	Configure aggregation parameters. Use the no version of the command to reset to default.	
Example	<b>Example (enable smac and dmac only)</b> # configure terminal (config)# aggregation mode smac dmac	

### 10.1.2. aggregation group

Description - Create and configure aggregation group. Each port can be a member of one aggregation group only and ports must be full duplex and have the same speed.

**aggregation group** <v\_uint> mode { [ active | on | passive ] }

**no aggregation group** <v\_uint>

Parameter	parameter	description
	<v_uint>	The aggregation group id
	[ active ]	Group operates in LACP active aggregation mode.
	[ on ]	Group operates in a static aggregation mode
	[ passive ]	Group operates in LACP passive aggregation mode
Default	N.A.	
Mode	Port List Interface Mode	
Usage	Configure aggregation group (add port to it). Use the no version of the command to remove the port from the aggregation group.	
Example	<b>Example (Configure port 1 to be a member of aggregation group 1 operation in active LACP mode)</b> # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# aggregation group 1 mode active	

### 10.1.3. lacp failover

Description - This parameter determines if the group will perform automatic link (re-)calculation when links with higher priority becomes available.

**lacp failover** { revertive | non-revertive }

**no lacp failover**

Parameter	parameter	description
	revertive	group will perform automatic link (re-)calculation
	non-revertive	group will not perform automatic link (re-)calculation
Default	Revertive failover is enabled.	
Mode	LLAG Mode	
Usage	Specify if the group will perform automatic link (re-)calculation. Use the no version of the command to revert to default.	
Example	<b>Example (set failover to non-revertive on interface LLAG 1)</b> # configure terminal (config)# interface llag 1 (config-llag)# lacp failover non-revertive	



### 10.1.4. lacp max-bundle

Description - This parameter determines the maximum number of active bundled LACP ports allowed in an aggregation.

**lacp max-bundle** <v\_uint>

**no lacp max-bundle**

Parameter	parameter	description
Parameter	<v_uint>	The aggregation group id
Default	Maximum number of active bundled ports 16.	
Mode	LLAG Mode	
Usage	Specify the maximum number of active bundled LACP ports allowed in an aggregation. Use the no version of the command to revert to default.	
Example	<b>Example (set failover to non-revertive on interface LLAG 1)</b> # configure terminal (config)# interface llag 1 (config-llag)# lacp max-bundle 10	

## 10.2. Aggregation Group Status view commands

### 10.2.1. show aggregation

Description- Display current status of ports in aggregation group and view parameters that contribute to the way Aggregation is done.

**show aggregation**

**show aggregation mode**

Parameter	parameter	description
Parameter	N.A	
Default	N.A	
Mode	EXEC Mode	
Usage	View the current aggregation status and parameters	
Example	<b>Example#1 (Display status of aggregation group)</b> # show aggregation	

### 10.3. LACP Configuration commands

The Link Aggregation Control protocol allows bundling several physical ports together to form a single logical link.

#### 10.3.1. lacp system-priority

Description - Set the system LACP priority

**lacp system-priority** <v\_1\_to\_65535>

**no lacp system-priority** <v\_1\_to\_65535>

Parameter	parameter	description
Parameter	<v_1_to_65535>	Priority value, lower means higher priority
Default	System priority 32768	
Mode	Global Configuration Mode	
Usage	Configure LACP system priority. Use the no version of the command to revert to default.	
Example	<p><b>Example#1 (set lacp system priority to 16384)</b>            # configure terminal            (config)# lacp system-priority 16384</p> <p><b>Example#2 (set lacp system priority to default)</b>            # configure terminal            (config)# no lacp system-priority 1</p>	

#### 10.3.2. lacp port-priority

Description- Set LACP priority of the port.

**lacp port-priority** <v\_1\_to\_65535>

**no lacp port-priority** <v\_1\_to\_65535>

Parameter	parameter	description
Parameter	<v_1_to_65535>	Priority value, lower means higher priority
Default	Port priority 32768	
Mode	Port List Interface Mode	
Usage	Configure LACP system priority. Use the no version of the command to revert to default.	
Example	<p><b>Example#1 (set lacp priority to 16384 for port#1)</b>            # configure terminal            (config)# interface GigabitEthernet 1/1            (config-if)# lacp port-priority 16384</p> <p><b>Example#2 (set lacp priority to default for port#1)</b>            # configure terminal            (config)# interface GigabitEthernet 1/1            (config-if)# no lacp port-priority 1</p>	

### 10.3.3. lacp timeout

Description- Specifies time period between BPDU transmissions.

**lacp timeout** { fast | slow }

**no lacp timeout** { fast | slow }

Parameter	parameter	description
Parameter	fast	Transmit BPDU each second (fast timeout)
	slow	Transmit BPDU each 30th second (slow timeout)
Default	Fast	
Mode	Port List Interface Mode	
Usage	Set the LACP timeout, i.e. how fast to transmit BPDUs, once a sec or once each 30 sec.	
Example	<p><b>Example#1 (set lacp timeout to slow for port#1)</b>  # configure terminal  (config)# interface GigabitEthernet 1/1  (config-if)# lacp timeout slow</p> <p><b>Example#1 (set lacp timeout to default (fast) port#1)</b>  # configure terminal  (config)# interface GigabitEthernet 1/1  (config-if)# no lacp timeout slow</p>	

## 10.4. LACP View commands

### 10.4.1. show lacp system-id

Description -Display local system priority and MAC address which forms the local LACP System ID

**show lacp system-id**

Parameter	parameter	description
Parameter	N.A	
Default	N.A	
Mode	EXEC Mode	
Usage	Display local system priority and MAC address	
Example	<p><b>Example</b>  #show lacp system-id</p>	

**10.4.2. show lacp internal details**

Description- Display status overview for LACP internal (local system) status for all ports that are part of the LACP group.

**show lacp internal details**

	parameter	description
Parameter	N.A	
Default	N.A	
Mode	EXEC Mode	
Usage	Display status overview for LACP ports	
Example	<b>Example</b> #show lacp internal details	

**10.4.3. show lacp neighbor details**

Description - Display status overview for the LACP neighbor status for all ports.

**show lacp neighbor details**

	parameter	description
Parameter	N.A	
Default	N.A	
Mode	EXEC Mode	
Usage	Display status overview for the LACP neighbor status for all ports.	
Example	<b>Example</b> #show lacp neighbor details	

**10.4.4. show lacp statistics details**

Description - Display overview for LACP statistics for all ports.

**show lacp statistics details**

	parameter	description
Parameter	N.A	
Default	N.A	
Mode	EXEC Mode	
Usage	Display overview for LACP statistics for all ports	
Example	<b>Example</b> #show lacp statistics details	

## 11. LLDP (LINK LAYER DISCOVERY PROTOCOL)

### 11.1. LLDP Configuration commands

The Link Layer Discovery Protocol allows stations to advertise their identity, capabilities and neighbors connected within the same network.

#### 11.1.1. LLDP parameters

Description - Configure LLDP parameters.

**lldp timer** <val>

**lldp holdtime** <val>

**lldp transmission-delay** <val>

**lldp reinit** <val>

Parameter	parameter	description
	timer<val>	Sets LLDP TX interval. The time between each LLDP frame transmitted in 5-32768 seconds
	holdtime<val>	Sets LLDP hold time. The neighbor switch will discard the LLDP information after 'hold time' multiplied with 'timer' 2-10seconds.
	transmission-delay<val>	Sets LLDP transmission-delay. The amount of time that the transmission of LLDP frames will be delayed after LLDP configuration has changed in 1-8192 seconds.
	reinit<val>	LLDP TX reinitialization delay in 1-10seconds
Default	Timer 30, Holdtime 4, transmission-delay 2, reinit 2	
Mode	Global Configuration Mode	
Usage	Configure LLDP parameters. Use the no version of the command to reset to default.	
Example	<b>Example</b> # configure terminal (config)# lldp timer 125 (config)# lldp holdtime 3 (config)# lldp transmission-delay 5 (config)# lldp reinit 5	

### 11.1.2. LLDP Interface configuration

Description - Configure LLDP parameters of the interface.

**lldp receive**

**lldp transmit**

**lldp cdp-aware**

**lldp trap**

**lldp tlv-select** { management-address | port-description | system-capabilities | system-description | system-name }

Parameter	parameter	description
Parameter	receive	Enable/Disable decoding of received LLDP frames.
	transmit	Enable/Disabled transmission of LLDP frames.
	cdp-aware	Configures if the interface shall be CDP aware (CDP discovery information is added to the LLDP neighbor table)
	trap	Configures if an SNMP trap shall be emitted when the LLDP neighbor table changes for the interface
	tlv-select	Enable/Disable transmission of optional TLVs
	Default	N.A.
Mode	Port List Interface Mode	
Usage	Enable LLDP parameters of the interface. Use the no version of the command to disable.	
Example	<p><b>Example</b></p> <pre># configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# lldp receive (config-if)# lldp cdp-aware (config-if)# lldp trap (config-if)# lldp tlv-select system-capabilities system-name</pre>	

## 11.2. LLDP View commands

### 11.2.1. show lldp neighbors

Description - Display status overview of all LLDP neighbors.

**show lldp neighbors** [ interface <port\_type> [ <v\_port\_type\_list> ] ]

Parameter	parameter	description
	<port_type>	Gigabit Ethernet port
	<v_port_type_list>	Port list 1/1-11
Default	N.A	
Mode	EXEC Mode	
Usage	Display status overview of all LLDP neighbors	
Example	<b>Example</b> #show lldp neighbors	

### 11.2.2. show lldp statistics

Description - Display status overview of all LLDP traffic.

**show lldp statistics** [ interface <port\_type> [ <v\_port\_type\_list> ] ]

Parameter	parameter	description
	<port_type>	Gigabit Ethernet port
	<v_port_type_list>	Port list 1/1-11
Default	N.A	
Mode	EXEC Mode	
Usage	Display status overview of all LLDP neighbors	
Example	<b>Example</b> #show lldp statistics	

## 12. PRIVATE VLAN / PORT ISOLATION

### 12.1. Private VLAN configuration commands

Private VLAN (has nothing to do with traditional VLAN) filters outgoing destination port traffic. Packet received on port X can be send only to destination ports which are marked as part of port X group.

#### 12.1.1. pvlan

Description - Add or remove a port from a PVLAN

**pvlan** <range\_list>

**no pvlan** <range\_list>

Parameter	parameter	description
Parameter	<range_list>	List of PVLANS. Range is from 1 to number of ports.
Default	N.A.	
Mode	Port List Interface Mode	
Usage	Add port to PVLAN. Use the no version of the command to remove the port from PVLAN.	
Example	<b>Example (Add port 1 to PVLAN 1,2 and 3 and then remove it from PVLAN 2)</b> # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# pvlan 1-3 (config-if)# no pvlan 2	

### 12.2. Private VLAN view commands

#### 12.2.1. show pvlan

Description- View the PVLAN configuration information.

**show pvlan** [<range\_list>]

Parameter	parameter	description
Parameter	<range_list>	List of PVLANS. Range is from 1 to number of ports.
Default	N.A	
Mode	EXEC Mode	
Usage	Display PVLAN configuration	
Example	<b>Example</b> #show pvlan	



## 12.3. Port Isolation configuration commands

Isolated ports are prevented from sending packets to each other. However, they can communicate normally with all the other Switch ports.

### 12.3.1. pvlan isolation

Description - Add the port to isolation group.

**pvlan isolation**

**no pvlan isolation**

Parameter	parameter	description
Parameter	N.A	
Default	N.A.	
Mode	Port List Interface Mode	
Usage	Add port to isolation group. Use the no version of the command to remove the port from isolation group.	
Example	<b>Example (Add port 1 isolation group)</b> # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# pvlan isolation	

## 12.4. Port Isolation view commands

### 12.4.1. show pvlan isolation

Description - View port isolation configuration

**show pvlan isolation** [ interface <port\_type\_list> ]

Parameter	parameter	description
Parameter	<port_type_list>	List of Port ID, ex, GigabitEthernet 1/1,3-5
Default	N.A	
Mode	EXEC Mode	
Usage	Display port isolation configuration	
Example	<b>Example (show port isolation configuration for port 2)</b> #show pvlan isolation interface GigabitEthernet 1/2 <b>Example (show port isolation configuration for all ports)</b> #show pvlan isolation	

## 13. LOOP PROTECTION

### 13.1. Loop protection configuration commands

Loop protect feature can prevent Layer2 loops by sending loop protect protocol packets and shutting down interfaces in case they receive loop protect packets originated from themselves.

#### 13.1.1. loop-protect (general settings)

Description - Configure Loop protection general parameters.

**loop-protect**

**no loop-protect**

**loop-protect transmit-time <t>**

**no loop-protect transmit-time**

**loop-protect shutdown-time <t>**

**no loop-protect shutdown-time**

Parameter	parameter	description
	<b>transmit-time &lt;t&gt;</b>	Interval between each loop protection PDU sent on each port. Valid values are 1-10 seconds.
	<b>shutdown-time &lt;t&gt;</b>	Period for which the port will be kept disabled if a loop is detected. Valid values 0-604800 seconds (7 days). A value of 0 will keep the port disabled until the next device restart.
Default	Transmission time 5 seconds. Shutdown time 180 seconds.	
Mode	Global Configuration Mode	
Usage	Enable/Disable Loop protection (globally) and configure Loop protection parameters. Use the no version of the command to reset to default.	
Example	<b>Example (Enable Loop protection and set transmit time to 8 seconds, shutdown time to 500 seconds)</b> # configure terminal (config)# loop-protect (config)# loop-protect transmit-time 8 (config)# loop-protect shutdown-time 500	

### 13.1.2. loop-protect (port settings)

Description - Configure Loop protection parameters for the switch port

**loop-protect**

**no loop-protect**

**loop-protect action** { [ shutdown ] [ log ] }

**no loop-protect action**

**loop-protect tx-mode**

**no loop-protect tx-mode**

Parameter	parameter	description
Parameter	shutdown	Shutdown the port when the Loop is detected
	log	Log only when the Loop is detected
	<b>tx-mode</b>	Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.
Default	N.A	
Mode	Port List Interface Mode	
Usage	Enable/Disable Loop protection on a switch port and configure Loop protection parameters.	
Example	<b>Example (Enable Loop protection on port 1, set it to Shutdown and Log when the loop is detected and disable Tx mode)</b> # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# loop-protect (config-if)# loop-protect action shutdown log (config-if)# no loop-protect tx-mode	

## 13.2. Loop protection status view commands

### 13.2.1. show loop-protect

Description - View Loop protection status

**show loop-protect** [ interface <port\_type> [ <plist> ] ]

Parameter	parameter	description
Parameter	<port_type>	Gigabit Ethernet port
	<plist>	List of Port ID, ex, GigabitEthernet 1/1,3-5
Default	N.A	
Mode	EXEC Mode	
Usage	Display Loop protection configuration and status.	
Example	<b>Example (show Loop protection configuration for port 2)</b> #show loop-protect interface GigabitEthernet 1/2 <b>Example (show Loop protection configuration for all ports)</b> #show loop-protect	

## 14. IGMP (INTERNET GROUP MANAGEMENT PROTOCOL)

### 14.1. IGMP Snooping Configuration commands

Snooping is the process of listening to IGMP (Internet Group Management Protocol) network traffic to control delivery of IP multicast packets. Network switches supporting IGMP snooping listen to IGMP conversation between hosts and routers and maintain a map of the ports that the IP multicast traffic should go through, while filter the IP multicast traffic from other Switch ports which do not need those IP Multicast packets, conserving bandwidth on those links.

#### 14.1.1. ip igmp (global parameters)

Description - Enable/disable IGMP Snooping and configure global parameters

**ip igmp snooping**

**no ip igmp snooping**

**ip igmp unknown-flooding**

**no ip igmp unknown-flooding**

**ip igmp ssm-range** <v\_ipv4\_mcast> <ipv4\_prefix\_length>

**no ip igmp ssm-range**

**ip igmp host-proxy** [ leave-proxy ]

**no ip igmp host-proxy** [ leave-proxy ]

Parameter	parameter	description
	<b>snooping</b>	Enable Global IGMP Snooping. Use the no version of the command to disable.
	<b>unknown-flooding</b>	Enable unregistered IPMCv4 traffic flooding. Use the no version of the command to disable.
	<b>ssm-range</b>	Source-Specific Multicast range. Use the no version of the command to set to default (232.0.0.0/8)
	<v_ipv4_mcast>	Valid IPv4 multicast address
	<ipv4_prefix_length>	Prefix length ranges from 4 to 32
	<b>host-proxy</b>	Enable IGMP Proxy. Use the no version of the command to disable.
	[ leave-proxy ]	Enable IGMP Leave Proxy. Use the no version of the command to disable.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Enable/Disable IGMP Snooping on a switch and configure global parameters.	
Example	<b>Example (Enable IGMP Snooping, unregistered IPMCv4 traffic flooding, proxy and leave proxy )</b> # configure terminal (config)# ip igmp snooping (config)# ip igmp unknown-flooding (config)# ip igmp host-proxy (config)# ip igmp host-proxy leave-proxy	

**14.1.2. ip igmp snooping (port parameters)**

Description - Configure IGMP Snooping on a specific port.

**ip igmp snooping mrouter**

**no ip igmp snooping mrouter**

**ip igmp snooping immediate-leave**

**no ip igmp snooping immediate-leave**

**ip igmp snooping max-groups <throttling>**

**no ip igmp snooping max-groups**

Parameter	parameter	description
	<b>mrouter</b>	Multicast router port configuration. Specify which ports act as a router ports (lead toward Layer 3 multicast device or IGMP querier)
	<b>immediate-leave</b>	Enable/Disable Fast Leave on the port.
	<b>max-groups</b>	Maximum number of multicast groups to which a switch port can belong (default unlimited)
	<throttling>	Number of multicast groups 1-10.
Default	N.A	
Mode	Port List Interface Mode	
Usage	Configure IGMP Snooping parameters on a port.	
Example	<b>Example (Configure IGMP Snooping parameters on port 1)</b> # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# ip igmp snooping mrouter (config-if)# ip igmp snooping immediate-leave (config-if)# ip igmp snooping max-groups 5	

**14.1.3. ip igmp snooping (vlan parameters)**

Description- Configure IGMP Snooping on a VLAN.

**ip igmp snooping**

**no ip igmp snooping**

**ip igmp snooping querier** { election | address <v\_ipv4\_ucast> }

**no ip igmp snooping querier** { election | address }

**ip igmp snooping compatibility** { auto | v1 | v2 | v3 }

**ip igmp snooping priority** <cos\_priority>

**no ip igmp snooping priority**

**ip igmp snooping robustness-variable** <ipmc\_rv>

**no ip igmp snooping robustness-variable**

**ip igmp snooping query-interval** <ipmc\_qi>

**no ip igmp snooping query-interval**

**ip igmp snooping query-max-response-time** <ipmc\_qri>

**no ip igmp snooping query-max-response-time**

**ip igmp snooping last-member-query-interval** <ipmc\_lmqi>

**no ip igmp snooping last-member-query-interval**

**ip igmp snooping unsolicited-report-interval** <ipmc\_uri>

**no ip igmp snooping unsolicited-report-interval**

Parameter	parameter	description
	<b>snooping</b>	Enable IGMP Snooping on a VLAN interface. Use the no version of the command to disable.
	<b>querier</b> { election }	Enable to join IGMP Querier election in the VLAN. Use the no version of the command to disable.
	<b>querier</b> { address <v_ipv4_ucast> }	Define IPv4 unicast address as source address used in IP header for IGMP Querier election.
	<b>compatibility</b> { auto   v1   v2   v3 }	IGMP interface compatibility. Forced IGMPv1, IGMPv2, IGMPv3 or auto (compatible with IGMPv1, IGMPv2, IGMPv3)
	<b>priority</b> <cos_priority>	Interface CoS Priority 0-7 with default value 0.
	<b>robustness-variable</b> <ipmc_rv>	Allows tuning for the expected packet loss tolerance count from 1 to 255. Default value is 2.
	<b>query-interval</b> <ipmc_qi>	Query Interval in 1-31744 seconds. Default value is 125.
	<b>query-max-response-time</b> <ipmc_qri>	Query Response Interval in 0-31744 tenths of seconds. Default value is 100 in tenth of seconds.
	<b>last-member-query-interval</b> <ipmc_lmqi>	Last Member Query Interval in 0-31744 tenths of seconds. Default value is 10 in tenth of seconds (1 second).
	<b>unsolicited-report-interval</b> <ipmc_uri>	Unsolicited Report Interval in 0-31744 seconds. Default value is 1 second.
Default	N.A	

Mode	VLAN Interface Mode
Usage	Enable/Disable IGMP Snooping on a switch and configure global parameters.
Example	<p><b>Example (Enable IGMP Snooping on a VLAN 2 interface with CoS priority 5 and all other default parameters)</b></p> <pre># configure terminal (config)# interface vlan 2 (config-if)# ip igmp snooping (config-if)# ip igmp snooping priority 5</pre>

## 14.2. IGMP Snooping View commands

### 14.2.1. show ip igmp snooping group-database

Description - View IGMP Snooping Group Information and statistics.

**show ip igmp snooping** [ vlan <v\_vlan\_list> ] [ group-database [ interface <port\_type> [ <v\_port\_type\_list> ] ] [ sfm-information ] ] [ detail ]

Parameter	parameter	description
	<v_vlan_list>	VLAN identifier (VLAN ID)
	<port_type>	Gigabit Ethernet port
	<v_port_type_list>	List of Port ID, ex, GigabitEthernet 1/1,3-5
Default	N.A	
Mode	EXEC Mode	
Usage	Display IGMP Snooping Group Information.	
Example	<p><b>Example (show detailed IGMP Snooping Group Information for vlan 2)</b></p> <pre>#show ip igmp snooping vlan 2 group-database detail</pre> <p><b>Example (show detailed running information and statistics if IGMP Snooping)</b></p> <pre>#show ip igmp snooping detail</pre>	

### 14.2.2. show ip igmp snooping mrouter

Description - Display which ports act as a router ports and the status.

**show ip igmp snooping mrouter** [ detail ]

Parameter	parameter	description
	N.A	
Default	N.A	
Mode	EXEC Mode	
Usage	Display Multicast router port status in IGMP	
Example	<p><b>Example</b></p> <pre>#show ip igmp snooping mrouter detail</pre>	

## 15. PORT MIRRORING

### 15.1. Port mirroring configuration

Port Mirroring allows the user to mirror (duplicate) Rx/Tx/Both traffic from one or more ports to another dedicated debug port where a network analyzer can be attached to analyze the network traffic.

#### 15.1.1. monitor session

Description - Enable Port Mirroring

**monitor session** <session\_number = 1>

**no monitor session** <session\_number = 1>

	parameter	description
Parameter	<session_number= 1>	Mirror session number. Must set as 1
Default	N.A	
Mode	Global Configuration Mode	
Usage	Enable traffic mirroring from one or more ports to a dedicated mirroring port. Use the no version of the command to disable.	
Example	<b>Example (Enable port mirroring)</b> # configure terminal (config)# monitor session 1	



### 15.1.2. Port configuration

Description - Configure port mirroring parameters

**monitor session** <session\_number> [ **destination** { interface <port\_type> [ <di\_list> ] } | **source** { interface <port\_type> [ <si\_list> ] [ both | rx | tx ] | **cpu** [ both | rx | tx ] }

Parameter	parameter	description
	<session_number = 1>	Mirror session number. Must set as 1
	<b>destination</b>	Mirror destination port
	<port_type>	Port type in GigaEthernet
	<di_list>	Port ID, ex, 1/1
	<b>source</b>	Mirror source ports
	<si_list>	List of Port ID, ex, 1/1,3-5
	both	Received and transmitted frames are mirrored on the destination port.
	rx	Only received frames are mirrored to the destination port.
	tx	Only transmitted frames are mirrored to the destination port.
	<b>cpu</b>	Mirror source CPU
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure which Switch ports to mirror, and to which port to mirror it to. Please disable MAC address learning for the destination port.	
Example	<b>Example (Set port 11 as a destination port to mirror received frames only on ports 1-5 )</b> # configure terminal (config)# monitor session 1 destination interface GigabitEthernet 1/11 (config)# monitor session 1 source interface GigabitEthernet 1/1-5 rx (config)# monitor session 1	

#### NOTE:

**NOTE – Please disable MAC address learning to the port used to mirror the traffic of the monitored ports.**

**To do please select the port to be configured, and type the command: no mac address-table learning**

## 16. MAINTENANCE

### 16.1. Reset and Restore unit

#### 16.1.1. reload cold

Description – Command unit to perform software reset, turning Ethernet ports down and back up.

##### reload cold

###### NOTE:

Unit software reset may or may-not effect PoE power being delivered to PD devices.

Use the command “poe uninterruptible-power”, “no poe uninterruptible-power” to configure PoE power state during software reset cycle.

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to restart the unit	
Example	# reload cold	

#### 16.1.2. reload defaults keep-ip

Description – Command unit to restore its configuration to semi factory default (only running configuration), keeping unit IP and VLAN configuration unchanged, in order to maintain remote Network connectivity

###### NOTE:

NOTE - New semi factory default configuration isn't automatically saved. You must issue a command as “copy running-config startup-config” in order to make the new configuration change permanent.

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to restore to factory default but keep IP address unchanged.	
Example	# reload defaults keep-ip	

### 16.1.3. reload defaults

Description – restore unit to full factory default configuration (only running configuration)

#### reload defaults

##### NOTES:



**NOTE 1:** - New factory default configuration isn't automatically saved. You must issue a command as "copy running-config startup-config" in order to make the new configuration change permanent

**NOTE 2:** - Connection to the device may be lost unless remote user is connected on the same LAN or has direct access to the device over serial (USB virtual COMM)

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to restore to factory default	
Example	# reload defaults	

## 16.2. Unit Configuration

### 16.2.1. Download unit configuration to TFTP-Server

Description- copy unit running-config, startup-config or another configuration file stored inside the unit to remote TFTP-Server.

**copy** <running-config | startup-config | flash:configuration-file-name> tftp://<TFTP-Server IP>/<filename>

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to copy one of the unit configurations to TFTP Server.	
Example	<p><b>Example #1 – copy running configuration to TFTP Server under name test</b></p> <p><b>Example #2 - save unit running configuration file to TFTP Server under name "test"</b></p> <pre># copy running-config tftp://192.168.0.40/test</pre> <p><b>Example #2 – copy unit local configuration file named test1 to TFTP-Server under name "unit-test-config-file".</b></p> <pre>#copy flash:test1 tftp://192.168.0.40/unit-test-config-file</pre>	

### 16.2.2. Upload configuration file from TFTP-Server to unit

Description – Upload configuration file from TFTP Server to any configuration file stored inside the unit internal FLASH memory except default-configuration (which is read-only).


**copy** <tftp://server-IP/filename> running-config | startup-config | flash:<file-name>

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to upload unit configuration from TFTP Server to unit local file	
Example	<p><b>Example – Upload from TFTP-Server configuration file named test1 to unit running-configuration</b></p> <pre>copy tftp://192.168.0.40/test1 running-configc opy copy tftp://192.168.0.40/test flash:test1</pre> <p><b>Example #2 - upload configuration file "test" to running configuration#</b></p> <pre>copy tftp://192.168.0.40/test running-config</pre>	

### 16.2.3. Activate one of the already stored configuration files

Description – Select which configuration file already stored inside the unit FLASH to activate, replacing the running configuration. To view the list of possible configuration files, use the command **dir**.

#### NOTE:

 The activated configuration file will not be saved to startup-config automatically. Please use **copy running-config startup-config** command to save it.

**copy** flash:<file-name> running-config

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to activate one of the unit other locally stored configuration files	
Example	<b>Example #1 - activate configuration file “test”</b> # copy flash:test running-config	

### 16.2.4. Delete configuration

Description – Delete configuration file from flash. To check the files stored in flash use dir command.  
 delete <flash:filename>

## 16.3. Software update

### 16.3.1. Upload new version

Description – Upload a new software version to the Switch.

**firmware upgrade** <url\_file>

Parameter	parameter	description
	<url_file>	Specific character string that constitutes a reference to a resource. Syntax:<protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name> If the following special characters: space !"#\$%&'()*+,-./:;<=>?@[\\]^_{ }~ need to be contained in the input URL string, they should be percent-encoded.
Default	N.A	
Mode	EXEC	
Usage	Use this command to upgrade Switch software version.	
Example	<b>Example – download unit new software version from TFTP Server</b> # firmware upgrade tftp://192.168.0.40/new_image.mfi	

### 16.3.2. Select active Image

Description – Swap the active and alternative image

**NOTE:**



Backup software version is the one used before latest software update was performed. Please note that using this command again will switch to the new software version that was just uploaded.

#### firmware swap

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to activate alternative (backup) image	
Example	<b>Example – swap the active and alternative images</b> # firmware swap	

## 17. DIAGNOSTICS

### 17.1. View log file

Description – Show System Log Information. Please note that system log file starts clean after each Switch RESET.

**show logging** [ informational ] [ notice ] [ warning ] [ error ]

**show logging** <log\_id> [ switch <switch\_list> ]

Parameter	parameter	description
Parameter	informational	Severity 6: Informational messages
	notice	Severity 5: Normal but significant condition
	warning	Severity 4: Warning conditions
	error	Severity 3: Error conditions
	<log_id>	Message logging ID
	<switch_list>	List of switch ID (in a stacked system) ex, 1,3-5,7
Default	N.A	
Mode	EXEC mode	
Usage	Display SysLog server status and configuration and detailed logging messages.	
Example	<b>Example#1 – show all switch log messages</b> # show logging#show logging 10 switch 1 <b>Example#2 – show all log messages with severity level of “notice”</b> #show logging notice	

### 17.2. Ping

Description – Test network connectivity between the unit and the remote network device.

**ping ip** { <domain\_name> | <ip\_addr> } [ repeat <count> ] [ size <size> ]

**ping ipv6** { <domain\_name> | <ip\_addr> } [ repeat <count> ] [ size <size> ]

Parameter	parameter	description
Parameter	<domain_name>	Destination host name
	<ip_addr>	Destination IPv4 or IPv6 address
	repeat <count>	Number of PING requests sent. Packets: 1-60; Default is 5
	size <size>	Size (bytes): 2-1452; Default is 56 (excluding MAC, IP and ICMP headers)
Default	N.A	
Mode	EXEC mode	
Usage	Ping remote host	
Example	<b>Example ( ping my.computer.com 10 times with 100 bytes packets)</b> #ping ip my.computer.com repeat 10 size 100	

### 17.3. RJ45 Cable test

Description – Perform Ethernet cable diagnostics, reporting cable length on each one of the Ethernet four pairs

**verify** [ { interface <port\_type> [ <v\_port\_type\_list> ] } ]

Parameter	parameter	description
	<port_type>	Port type in GigaEthernet
	<v_port_type_list>	List of Port ID, ex, 1/1,3-5,7
Default	N.A	
Mode	EXEC mode	
Usage	Run cable diagnostics	
Example	<p><b>Example#1 - perform cable diagnostic on port 2</b></p> <pre>#verify interface GigabitEthernet 1/2</pre> <pre># verify interface GigabitEthernet 1/2 Starting VeriPHY - Please wait Interface          Pair A  Length  Pair B, Length  Pair C  Length  Pair D  Length ----- GigabitEthernet 1/2  OK     0       OK     0       short  0       short  0</pre> <p><b>Example#2 - perform cable diagnostic on all ports (may take a long time)</b></p> <pre>#verify</pre>	



## 17.4. View CPU Load

Description – Show CPU load. The load is measured as average over the last 100ms, 1sec and 10 seconds intervals.

**show system cpu status**

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to display cpu status	
Example	<pre># show system cpu status # show system cpu status   Average load in 100 ms : 0%   Average load in 1 sec : 0%   Average load in 10 sec : 0%</pre>	

### Revision History

Revision Level / Date	Para. Affected	Description
0.7	Whole Document	initial document

For support contact: [PoEsupport@microsemi.com](mailto:PoEsupport@microsemi.com)

Visit our web site at: [PoE Midspans, PoE Injectors & PoE Switches](#)