Supermicro Switch Configuration

CLI User's Guide

Volume 1

Revision 2.1

The information in this USER'S GUIDE has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, makes no commitment to update or to keep current the information in this manual, or to notify any person organization of the updates. Please Note: For the most up-to-date version of this manual, please see our web site at www.supermicro.com.

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software, if any, and documentation may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any medium or machine without prior written consent.

DISCLAIMER OF WARRANTY ON SOFTWARE AND MATERIALS. You expressly acknowledge and agree that use of the Software and Materials is at your sole risk. FURTHERMORE, SUPER MICRO COMPUTER INC. DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE SOFTWARE OR MATERIALS IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY SUPER MICRO COMPUTER INC. OR SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SHOULD THE SOFTWARE AND/OR MATERIALS PROVE DEFECTIVE, YOU (AND NOT SUPER MICRO COMPUTER INC. OR A SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICE, REPAIR, OR CORRECTION.

LIMITATION OF LIABILITY. UNDER NO CIRCUMSTANCES INCLUDING NEGLIGENCE, SHALL SUPER MICRO COMPUTER INC. BE LIABLE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES THAT RESULT FROM THE USE OR INABILITY TO USE THE SOFTWARE OR MATERIALS, EVEN IF SUPER MICRO COMPUTER INC. OR A SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Super Micro's total liability for all claims will not exceed the price paid for the hardware product.

Manual Revision 2.0.0
Release Date: 8/11/2020

Document Revision History

Date	Revision	Description
	1.0	Initial document.
	2.0	Upgraded document with new content and format
2020/11/19	2.1	Add 25G/100G interfaces and SMCPL100 related update

Contents

1 Introduction 18

1.1 Purpose 18

1.2 Scope 18

1.3 Document Conventions 18

1.4 Industry Standard CLI 18

1.5 Key Conventions 19

2 Command Line Interface 20

2.1 Context Sensitive Help 20

2.2 CLI command modes 22

3 System Commands 27

3.1 help 29

3.2 clear screen 30

3.3 enable 31

3.4 disable 33

3.5 configure terminal 34

3.6 configure 35

3.7 run script 36

3.8 listuser 37

3.9 lock 38

3.10 username 39

3.11 enable password 42

3.12 line 43

3.13 alias - replacement string 45

3.14 alias – interface | exec | configure 46

3.15 access-list provision mode 48

3.16 access-list commit 49

3.17 exec-timeout 50

3.18 logout 51

3.19 end 52

3.20 Exit 53

3.21 show privilege 54

3.22 show line 55

3.23 show aliases 56
3.24 show users 57
3.25 show history 58
3.26 password validate char 59
3.27 password validate uppercase 60
3.28 password validate lowercase 61
3.29 password validate numbers 62
3.30 password validate symbols 63
3.31 set minimum password length 64
3.32 show password validate rules 65
3.33 show minimum password length 66
3.34 password max-life-time 67
3.35 show password max-life-time 68
3.36 set cli pagination 69
3.37 coredump 70
3.38 show tech-support 72
3.39 show meminfo 73
3.40 set boot 74
3.41 show boot 75
3.42 reset-factory-default 76
3.43 show blade interfaces ..... **Error! Bookmark not defined.**
4 System Features 77
4.1 default mode 81
4.2 default restore-file 83
4.3 ip address 84
4.4 switchport 86
4.5 ip address - rarp/dhcp 88
4.6 login authentication 90
4.7 login authentication-default 92
4.8 authorized-manager ip-source 94
4.9 ip http port 98
4.10 set ip http 99
4.11 mtu 100

4.12 system mtu 102
4.13 bridge port-type 104
4.14 system-specific port-id 108
4.15 set custom-param 109
4.16 mac-addr 111
4.17 snmp trap link-status 112
4.18 Write 113
4.19 copy 115
4.20 copy startup-config 117
4.21 copy running-config startup-config 119
4.22 copy logs 120
4.23 firmware upgrade 122
4.24 copy - file 124
4.25 clock set 126
4.26 erase 128
4.27 cli console 129
4.28 flowcontrol 130
4.29 tunnel mode 132
4.30 tunnel checksum 134
4.31 tunnel path-mtu-discovery 135
4.32 tunnel udlr 137
4.33 shutdown - physical/VLAN/port-channel/tunnel Interface 138
4.34 debug interface 140
4.35 debug-logging 142
4.36 incremental-save 143
4.37 auto-save trigger 144
4.38 set switch maximum - threshold 145
4.39 set switch temperature - threshold 147
4.40 set switch power - threshold 149
4.41 mac-learn-rate 151
4.42 system contact 153
4.43 system location 154
4.44 clear interfaces - counters 155

4.45 clear counters 157
4.46 show ip interface 159
4.47 show authorized-managers 161
4.48 show interfaces 162
4.49 show interfaces - counters 168
4.50 show system-specific port-id 171
4.51 show custom-param 172
4.52 show interface mtu 173
4.53 show interface bridge port-type 175
4.54 show nvram 177
4.55 show env 180
4.56 show system information 183
4.57 show flow-control 185
4.58 show debug-logging 187
4.59 show debugging 188
4.60 show clock 190
4.61 show running-config 191
4.62 show http server status 199
4.63 show system acknowledgement 200
4.64 show mac-learn-rate 202
4.65 port-isolation in_vlan_ID 203
4.66 show port-isolation 204
4.67 private-vlan mapping 206
4.68 audit-logging 207
4.69 audit-logging filename 208
4.70 audit-logging filesize 209
4.71 audit-logging reset 210
4.72 show config log 211
4.73 hol blocking prevention 212
4.74 internal-lan 213
4.75 show internal-lan 214
4.76 show iftype protocol deny table 215
4.77 clear line vty 216

4.78 tunnel hop-limit 217
4.79 login block-for 218
4.80 audit-logging logsize-threshold 219
4.81 feature telnet 220
4.82 show telnet server 221
4.83 show audit 222
4.84 set http authentication-scheme 223
4.85 set http redirection enable 224
4.86 http redirect 225
4.87 show http authentication-scheme 226
4.88 show http redirection 227
4.89 ENTITY MIB 228
4.90 set entity physical-index 229
4.91 show entity logical 232
4.92 show entity physical 233
4.93 show entity lp-mapping 235
4.94 show entity alias-mapping 236
4.95 show entity phy-containment 237
4.96 set hitless-restart enable 240
4.97 speed 241
4.98 automatic-port-create 242
4.99 port-type providerInstancePort 244
4.100 sleep 245
4.101 rate-limit pause 246
4.102 cpu controlled learning 247
4.103 traffic-separation control 248
4.104 mdix auto 250
4.105 set port 251
4.106 config-restore 252
4.107 set switch-name 253
4.108 packet receive index 254
4.109 packet send index port 255
4.110 packet send index value 256

4.111 show packetsend index 257
4.112 show packetreceive index 258
4.113 set mirroring 259
4.114 default exec-timeout 260
4.115 ip unnumbered 261
4.116 clear http server statistics 264
4.117 show license 265
4.118 install license 266
4.119 uninstall license 268
4.120 copy debug-files 269
4.121 multiplex 270
4.122 ip mtu 271
4.123 aaa authentication login ascii-authentication 272
4.124 aaa authentication login default group 273
4.125 aaa group server tacacs+ 275
4.126 server 276
4.127 ztp 277
5 RADIUS 278
5.1 radius-server host 279
5.2 debug radius 281
5.3 show radius server 282
5.4 show radius statistics 284
6 TACACS 286
6.1 tacacs-server host 287
6.2 tacacs use-server address 289
6.3 tacacs-server retransmit 290
6.4 aaa authorization 291
6.5 aaa accounting 292
6.6 debug tacacs 293
6.7 show tacacs 294
6.8 show accounting 296
7 SSH 297
7.1 ip ssh 298

7.2 ssh 300
7.3 debug ssh 301
7.4 show ip ssh 303
7.5 ip ssh transport-max-allowed bytes 304
7.6 ip ssh pubkey-chain 305
7.7 ssh server-address 306
7.8 show ssh-configurations 307
8 SSL 308
8.1 ip http secure 309
8.2 ssl gen cert-req algo rsa sn 312
8.3 ssl server-cert 313
8.4 debug ssl 314
8.5 show ssl server-cert 316
8.6 show ip http secure server status 318
8.7 version 319
9 SNTP 322
9.1 sntp 324
9.2 set sntp client 326
9.3 set sntp client version 327
9.4 set sntp client addressing mode 328
9.5 set sntp client port 330
9.6 set sntp client clock-format 331
9.7 set sntp client time zone 332
9.8 set sntp client clock-summer-time 333
9.9 set sntp client authentication-key 335
9.10 set sntp unicast-server auto-discovery 337
9.11 set sntp unicast-poll-interval 338
9.12 set sntp unicast-max-poll-timeout 339
9.13 set sntp unicast-max-poll-retry 340
9.14 set sntp unicast-server 341
9.15 set sntp broadcast-mode send-request 343
9.16 set sntp broadcast-poll-timeout 344
9.17 set sntp broadcast-delay-time 345

9.18 set sntp multicast-mode send-request 346
9.19 set sntp multicast-poll-timeout 347
9.20 set sntp multicast-delay-time 348
9.21 set sntp multicast-group-address 349
9.22 set sntp manycast-poll-interval 350
9.23 set sntp manycast-poll-timeout 351
9.24 set sntp manycast-poll-retry-count 352
9.25 set sntp manycast-server 353
9.26 show sntp clock 354
9.27 show sntp status 355
9.28 show sntp unicast–mode status 357
9.29 show sntp broadcast–mode status 359
9.30 show sntp multicast—mode status 360
9.31 show sntp manycast–mode status 361
9.32 debug sntp 362
9.33 show sntp statistics 364
9.34 show clock properties 365
9.35 clock time source 366
9.36 no clock time source 367
10 SNMPv3 368
10.1 enable snmpsubagent 370
10.2 disable snmpsubagent 372
10.3 enable snmpagent 373
10.4 disable snmpagent 374
10.5 snmp community index 375
10.6 snmp group 377
10.7 snmp access 379
10.8 snmp engineid 381
10.9 snmp proxy name 382
10.10 snmp mibproxy name 384
10.11 snmp view 386
10.12 snmp targetaddr 388
10.13 snmp targetparams 390

10.14 snmp user 393
10.15 snmp notify 395
10.16 snmp filterprofile 397
10.17 snmp-server enable traps snmp authentication 399
10.18 snmp-server trap udp-port 400
10.19 snmp-server trap proxy-udp-port 401
10.20 snmp agent port 402
10.21 snmp tcp enable 403
10.22 snmp trap tcp enable 404
10.23 snmp-server tcp-port 405
10.24 snmp-server trap tcp-port 406
10.25 snmp-server enable traps 407
10.26 show snmp agentx information 408
10.27 show snmp agentx statistics 409
10.28 show snmp 411
10.29 show snmp community 413
10.30 show snmp group 414
10.31 show snmp group access 416
10.32 show snmp engineID 418
10.33 show snmp proxy 419
10.34 show snmp mibproxy 421
10.35 show snmp viewtree 422
10.36 show snmp targetaddr 423
10.37 show snmp targetparam 424
10.38 show snmp user 426
10.39 show snmp notif 428
10.40 show snmp inform statistics 429
10.41 show snmp-server traps 430
10.42 show snmp-server proxy-udp-port 431
10.43 show snmp tcp 432
10.44 show snmp filter 433
10.45 snmpset mib 434
10.46 snmpget mib 436

10.47 snmpgetnext mib 437
10.48 snmpwalk mib 438
10.49 snmp filter trap 439
10.50 show mib oid 440
10.51 show mib name 441
11 Syslog 442
11.1 Logging 444
11.2 logging synchronous 447
11.3 mailserver 449
11.4 sender mail-id 451
11.5 cmdbuffs 452
11.6 clear logs 453
11.7 syslog mail 454
11.8 syslog local storage 455
11.9 syslog filename-one 456
11.10 syslog filename-two 457
11.11 syslog filename-three 458
11.12 syslog relay - port 459
11.13 syslog profile 460
11.14 logging-file 461
11.15 logging server 462
11.16 syslog relay 464
11.17 syslog relay transport type 465
11.18 show logging 466
11.19 show email alerts 468
11.20 show syslog role 469
11.21 show syslog mail 470
11.22 show syslog localstorage 471
11.23 show logging-file 472
11.24 show logging-server 474
11.25 show mail-server 475
11.26 show syslog relay-port 476
11.27 show syslog profile 477

11.28 show syslog relay transport type 478
11.29 show syslog file-name 479
11.30 show syslog information 480
11.31 smtp authentication 481
11.32 snmp trap syslog-server-status 482
12 TCP 483
12.1 show tcp statistics 484
12.2 show tcp connections 488
12.3 show tcp listeners 492
12.4 show tcp retransmission details 494
12.5 tcp max retries 496
13 UDP 497
13.1 show udp statistics 498
13.2 show udp connections 500
14 L2 DHCP Snooping 502
14.1 ip dhcp snooping - Global Command 503
14.2 ip dhcp snooping verify mac-address 504
14.3 ip dhcp snooping - VLAN Interface Command 505
14.4 ip dhcp snooping trust 506
14.5 show ip dhcp snooping globals 507
14.6 show ip dhcp snooping vlan 508
14.7 debug ip dhcp snooping 510
15 IPDB 511
15.1 ip binding 512
15.2 ip source binding 514
15.3 ip verify source 516
15.4 show ip binding 517
15.5 show ip source binding 518
15.6 show ip binding counters 520
15.7 show ip verify source 521
15.8 debug ip binding database 523
16 STP 524
16.1 STP Commands Common for RSTP and MSTP 525

16.2 shutdown spanning-tree 527
16.3 spanning-tree 530
16.4 spanning-tree Mode 532
16.5 spanning-tree compatibility 536
16.6 spanning-tree timers 538
16.7 spanning-tree transmit hold-count 541
16.8 clear spanning-tree counters 543
16.9 spanning-tree pathcost dynamic 546
16.10 spanning-tree priority 548
16.11 spanning-tree auto-edge 550
16.12 spanning-tree - Properties of an interface 551
16.13 spanning-tree portfast - disable | trunk 555
16.14 spanning-tree portfast - bpdufilter default | bpduguarddefault | default 556
16.15 spanning-tree restricted-role 558
16.16 spanning-tree restricted-tcn 560
16.17 spanning-tree layer2-gateway-port 562
16.18 spanning-tree bpdu-receive 564
16.19 spanning-tree bpdu-transmit 566
16.20 spanning-tree loop-guard 568
16.21 spanning-tree – Pseudoroot configuration 570
16.22 debug spanning-tree 572
16.23 clear spanning-tree detected protocols 575
16.24 show spanning-tree - Summary, Blockedports, Pathcost, Redundancy 577
16.25 show spanning-tree detail 586
16.26 show spanning-tree active 591
16.27 show spanning-tree interface 595
16.28 show spanning-tree root 603
16.29 show spanning-tree bridge 606
16.30 show spanning-tree – layer 2 gateway port 609
16.31 show customer spanning-tree 611
16.32 spanning-tree forwarddelay optimization alternate-role 615
17 MSTP 617
17.1 spanning-tree mst max-hops 618

17.2 spanning-tree mst configuration 620
17.3 spanning-tree mst max-instance 621
17.4 spanning-tree mst root 622
17.5 spanning-tree mst forward-time 624
17.6 spanning-tree mst max-age 626
17.7 name 628
17.8 revision 629
17.9 Instance 630
17.10 spanning-tree mst- Properties of an interface for MSTP 632
17.11 spanning-tree mst hello-time 635
17.12 show spanning-tree mst - CIST or specified mst Instance 637
17.13 show spanning-tree mst configuration 640
17.14 show spanning-tree mst - Port Specific Configuration 642
17.15 spanning-tree flush-interval 645
17.16 spanning-tree flush-indication-threshold 646
18 LLDP 648
18.1 shutdown lldp 650
18.2 set lldp 653
18.3 lldp transmit-interval 655
18.4 lldp holdtime-multiplier 656
18.5 lldp reinitialization-delay 657
18.6 lldp tx-delay 658
18.7 lldp notification-interval 659
18.8 lldp chassis-id-subtype 660
18.9 clear lldp counters 662
18.10 clear lldp table 663
18.11 lldp transmit / receive 664
18.12 lldp notification 666
18.13 lldp tlv-select basic-tlv 668
18.14 lldp port-id-subtype 670
18.15 lldp tlv-select dot1tlv 672
18.16 lldp tlv-select dot3tlv 674
18.17 debug lldp 676

18.18 show lldp 679
18.19 show lldp interface 681
18.20 show lldp neighbors 683
18.21 show lldp traffic 689
18.22 show lldp local 691
18.23 show lldp errors 696
18.24 show lldp statistics 697
18.25 lldp dest-mac 698
18.26 set lldp version 699
18.27 lldp txCreditMax 700
18.28 lldp MessageFastTx 701
18.29 lldp txFastInit 702
18.30 show lldp peer 703
Contacting Supermicro 705

1 Introduction

SuperMicro Intelligent Switch (SMIS) is a software for managed Layer 2/Layer 3 switches, which performs switching between Ethernet ports at wire speed. SMIS provides the basic bridging functionality and also offers advanced features such as link aggregation, GVRP/GMRP, IGMP Snooping and Network Access Control.

1.1 Purpose

This document describes in detail the Base CLI commands supported by SMIS. It is intended to be a reference manual for users and system administrators who will configure Supermicro switches through the CLI interface.

1.2 Scope

The scope of this document is limited to SMIS release 2.0.0 and above. This document details all the Base CLI commands provided by the SMIS software. Commands that are not applicable for a specific hardware platform are indicated wherever necessary.

1.3 Document Conventions

- The syntax of the CLI command is given in **`Courier New 10 bold orange`**.
- Elements in (< >) indicate the field required as input along with a CLI command, for example, < integer (100-1000)>.
- Elements in square brackets ([]) indicate optional fields for a command.
- Text in {} refers to either or group for the tokens given inside separated by a | symbol.
- The CLI command usage is given in **`Courier New 10 regular`**.
- Outputs and messages for CLI commands are given in `Courier New 10 regular blue`.
- The no form of the command resets a particular configuration to its default value or revokes the effect. This is explicitly explained in the description of the commands for which it is applicable.
- Any action that can change the switch configuration, conditionals and requirements for a command and information associated with significant details and functionality of a command is listed using the symbol.

1.4 Industry Standard CLI

CLI commands are focused on performing specific operations. In order to provide a consistent, composable user experience, the CLI commands of the protocols and solutions, have been modified to adhere to the Industry

Standard CLI syntax. This enhancement is available for the code base using release after SMIS 2.0.0.

1.5 Key Conventions

Keyboard Shortcuts

- **Up Arrow / Down Arrow** - Displays the previously executed command.
- **Backspace / Ctrl + H** - Removes a single character.
- **TAB** - Completes a command without typing the full word.
- **Left Arrow / Right Arrow** - Traverses the current line.

Others

- ? - helps to list the available command
- Q - exits and returns to the SMIS prompt
- History - displays the command history list

2 Command Line Interface

This section describes the configuration of Supermicro **SMIS** using the CommandLine Interface.

The Command Line Interface (CLI) can be used to configure the Intelligent Switch Solution from a console attached to the serial port of the switch or from a remote terminal using TELNET.

The **SMIS** CLI supports a simple login authentication mechanism. The authentication is based on a user name and password provided by the user during login. The user "ADMIN" is created by default with a unique password. The unique password is printed on the label with the switch serial number and MAC address.

A new user can be created or an existing user can be deleted, and the own password or password of the other users can be modified, only if login as an ADMIN user.

When **SMIS** is started, the user name and password has to be given at the login prompt to access the CLI shell:

```
Supermicro Switch
SMIS Login: ADMIN
Password: **********
SMIS>
```

The **user-exec** mode is now available to the user. CLI command modes provide a detailed description of the various modes available for SMIS.

The command prompt always displays the current mode.

CLI commands need not be fully typed. The abbreviated forms of CLI commands are also accepted by the SMIS CLI. For Example, commands like "show ip global config" can be typed as "sh ip gl co".

CLI commands are case insensitive.

CLI commands will be successful only if the dependencies are satisfied for a particular command that is issued. The general dependency is that the module specific commands are available only when the respective module is 'enabled'. Appropriate error messages will be displayed, if the dependencies are not satisfied.

The Ethernet type of an interface is determined during System Startup. While configuring interface-specific parameters, its Ethernet type needs to be specified correctly. A fastethernet interface cannot be configured as a gigabit-ethernet interface and vice-versa.

2.1 Context Sensitive Help

SMIS CLI framework offers context sensitive help; The user can type a question mark (?) anytime during a session to get help. The help can be invoked in several ways. It is not displayed as a whole and is available only for the specific token from where it is invoked.

Examples of possible scenarios are given below.

1. User keys in a character followed immediately by a question mark (?). This displays the current possible tokens without help string.

```
SMIS(config)# bo?

bootfile
```

2. User enters a keyword at the command prompt and enters a question mark (?) after hitting a space. This displays the next possible tokens along with the corresponding help string..

```
SMIS(config)# service ?

dhcp              DHCP related configuration

dhcp-relay        DHCP relay related

configuration dhcp-server     DHCP server

related configuration


timestamps        Timestamp configuration for
logged messages
```

Some of the basic concepts implemented for the context sensitive help are:

- The next possible tokens are listed only in the lexical order and not in the order as available in the syntax or command structure.
- All possible tokens are listed along with the help string, even though the command is ambiguous. Any ambiguous command errors and value range errors are taken care only during the execution of the command.
- The help tokens provided within <> brackets denote that the user should input values of specified format. For Example, <string(32)> represents that the user should input a string of size varying from 1 to 32.
- The help tokens provided within () brackets denotes that the user should input only the values represented. For Example, (1-4094) represents that the user should input value within the mentioned range alone.
- The format is directly provided as help token for some non-keyword such as IP address, IP mask , MAC address and so on. For Example, aa:aa:aa:aa:aa:aa represents that a MAC address of this format should be provided.
- Only the most commonly used format is provided as help token for some non-keywords such as IPv6 address. But the command supports most of the valid formats. For Example, AAAA::BBBB represents the IPv6 address, but the command will accept the format AAAA:B::BBBB.
- The help token <CR> along with help string explaining the operation of the command is displayed, if the command can be executed at that point (errors are handled only during the execution).

2.2 CLI command modes

The following table format lists the different CLI command modes. Depending on the CLI mode, your product prompt will be specific. This can be changed by the end user.

For Example; If your product label is ABC and the command mode is Global Configuration, the prompt display will be **`ABC (config)`**

Command Mode	Access Method	Prompt	Exit method
User EXEC	This is the initial mode to start a session.	**switch name>**	The logout method is used.
Privileged EXEC	The User EXEC mode command **`enable`** is used to enter the Privileged EXEC mode.	**switch name#**	To return from the Privileged EXEC mode to User EXEC mode the disable command is used.
Global Configuration	The Privileged EXEC mode command **`configure terminal`** is used to enter the Global Configuration mode	**switch name(config)#**	To exit to the Privileged EXEC mode the **`end`** command is used.
Interface Configuration	The Global Configuration mode command **`interface <interface-type> <interface- id>`** is used to enter the interface configuration mode	**switch name(config-if)#**	To exit to the Global Configuration mode the exit command is used and to exit to the Privileged EXEC mode the end command is used.
Interface Range Mode	The Global Configuration mode command **interface range ({<interface-type> <slot/port-port>} {vlan <vlan-id(1-4069)> - <vlan-id(1-4069)>}** is used to enter the interface range mode	**switch name(config-if-range)#**	To exit to the Global Configuration mode the **`exit`** command is used and to exit to the Privileged EXEC mode the **`end`** command is used.
Config-VLAN	The Global configuration mode command **`vlan vlan- id`** is used to enter the Config-VLAN mode	**switch name (config-vlan)#**	To exit to the Global Configuration mode the **`exit`** command is used and to exit to the Privileged EXEC mode the **`end`** command is used.
Line Configuration	The global configuration mode command **`line`** is used to enter the Line Configuration	**switch name (config-line)#**	To exit to the Global Configuration mode the **`exit`** command is used and to exit to the Privileged EXEC mode the **`end`** command is used.

User EXEC Mode

After logging into the device, the user is automatically in the User EXEC mode. In general, the User EXEC commands are used to temporarily change terminal settings, perform basic tests and list system information.

Privileged EXEC Mode

Because many of the privileged commands set operating parameters, privileged access is password protected to prevent unauthorized use. The password is not displayed on the screen and is case sensitive. The Privileged EXEC mode prompt is the device name followed by the pound (#) sign.

Global Configuration Mode

Global Configuration commands apply to features that affect the system as a whole, rather to any specific interface.

Interface Configuration Mode

To enter into Interface configuration mode from the Global Configuration mode, **`interface <interface-type><interface-id>`** command is used. To exit to the global configuration mode the **`exit`** command is used and to exit to the privileged EXEC mode the **`end`** command is used.

The interface can be:

- cx-ethernet – A version of LAN standard architecture that supports data transfer upto 100 Gigabits per second.
- qx-ethernet – A version of LAN standard architecture that supports data transfer upto 40 Gigabits per second.
- fx-ethernet – A version of LAN standard architecture that supports data transfer upto 50 Gigabits per second.
- extreme-ethernet – A version of LAN standard architecture that supports data transfer upto 10 Gigabits per second.
- gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabits per second.

Physical Interface Mode

The Physical Interface mode is used to perform interface specific operations. To return to the global configuration mode the **`exit`** command is used.

Port Channel Interface Mode

The Port Channel Interface mode is used to perform port-channel specific operations. To return to the global configuration mode the **`exit`** command is used.

VLAN Interface Mode

The VLAN Interface mode is used to perform L3-IPVLAN specific operations. To return to the global configuration mode the **`exit`** command is used.

Management Interface Mode

The management Interface mode is used to perform OOB interface specific operations. To return to the global configuration mode the **`exit`** command is used.**Interface Range Mode**

To enter into Interface range mode from the Global Configuration mode, **interface range ({ <interface-type> <slot/port-port>}**

{vlan <vlan-id(1-4094)> - <vlan-id(2-4094)>}) command is used. To exit to the global configuration mode the **exit** command is used and to exit to the privileged EXEC mode

Config-VLAN Mode

This mode is used to perform VLAN specific operations. To enter into Config-VLAN mode from the global configuration mode, **vlan vlan-id** command is used. To return to the global configuration mode the **exit** command is used.

Line Configuration Mode

Line configuration commands modify the operations of a terminal line. These commands are used to change terminal parameter settings line by line or range of lines. To enter into Line Configuration mode from the global configuration mode, **line** command is used. To exit to the Global Configuration mode the **exit** command is used and to exit to the Privileged EXEC mode the **end** command is used.

Protocol Specific Modes

The following are the specified protocol modes;

- VRRP Router Configuration Mode
- VRRP Interface Configuration Mode
- DHCP Pool Configuration Mode
- SNTP Configuration Mode
- MSTP Configuration mode
- DiffSrv ClassMap Configuration mode
- DiffSrv Policy-Map Configuration Mode
- ACL Standard Access List Configuration Mode
- ACL Extended Access List Configuration Mode
- ACL MAC Configuration Mode
- CEE-Map Configuration Mode

VRRP Router Configuration Mode

This mode is used for configuring the virtual router. To enter to this mode, the command router vrrp from the Global configuration mode is used. To exit to the Global Configuration mode the **exit** command is used and to exit to the Privileged EXEC mode the **end** command is used.

VRRP Interface Configuration Mode

VRRP interface config mode is used to configure VRRP interfaces. To enter into this mode, **interface Vlan <vlan id>** command from VRRP router config mode is used. To exit to the Virtual Router Configuration mode the **exit** command is used and to exit to the Privileged EXEC mode the **end** command is used.

DHCP Pool Configuration Mode

This mode is used to configure the network pool / host configurations of a subnet pool.

The Global configuration mode command **ip dhcp pool <integer(1-2147483647)>** creates a DHCP Server address pool and places the user in

DHCP pool configuration mode. The prompt seen at this mode is **Your Product(dhcp-config)#**.

To return to the global configuration mode the **exit** command is used.

SNTP Configuration Mode

SNTP Configuration mode is used to configure SNTP parameters. To enter into this mode, **sntp** command from the Global Configuration mode is used. The prompt seen at this mode is **Your Product(config-sntp)#**. To exit to the Global Configuration mode the **exit** command is used and to exit to the Privileged EXEC mode the **end** command is used.

MSTP Configuration mode

This mode is used to configure the MSTP specific parameters for the switch. The Global configuration mode command **spanning tree mst configuration** is used to enter the MSTP Configuration mode and. the prompt seen at this mode is **Your Product (config-mst)#.**

To return to the global configuration mode the **exit** command is used.

DiffSrv ClassMap Configuration mode

The class-map global configuration command creates a class map to be used for matching the packets to the class whose index is specified and to enter the class-map configuration mode The Global configuration mode **command class-map <short(1-65535)>** is used to enter the DiffSrv ClassMap Configuration mode and. the prompt seen at this mode is **Your Product (config-cmap)#**.

To return to the global configuration mode the **exit** command is used.

DiffSrv Policy-Map Configuration Mode

In the Policy-Map Configuration mode the user can create or modify a policy map.

The Global configuration mode command **policy-map <short(1-65535)>** is used to enter the DiffSrv Policy Map Configuration mode and the prompt seen at this mode is **Your Product (config-pmap)#.**

To return to the global configuration mode the **exit** command is used.

ACL Standard Access List Configuration Mode

Standard access lists create filters based on IP address and network mask only (L3 filters only).

The Global configuration mode command **ip access-list standard <(1-1000)** creates IP ACLs and is used to enter the ACL Standard Access List Configuration mode. The prompt seen at this mode is **Your Product (config-std-nacl)#.**

To return to the global configuration mode the **exit** command is used.

ACL Extended Access List Configuration Mode

The Extended Access lists enables to specify filters based on the type of protocol, range of TCP/UDP ports as well as IP address and network mask (Layer 4 filters).

The Global configuration mode command **`ip access-list extended <(1001-65535)>`** is used to enter the ACL Extended Access List Configuration mode and the prompt seen at this mode is **`Your Product (config-ext-nacl)#.`**

To return to the global configuration mode the **`exit`** command is used.

ACL MAC Configuration Mode

The MAC access-list global configuration command creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user.

The Global configuration mode command **`mac access-list extended <(1-65535)>`** is used to enter the ACL MAC Configuration mode and the prompt seen at this mode is **`Your Product (config-ext-macl)#.`**

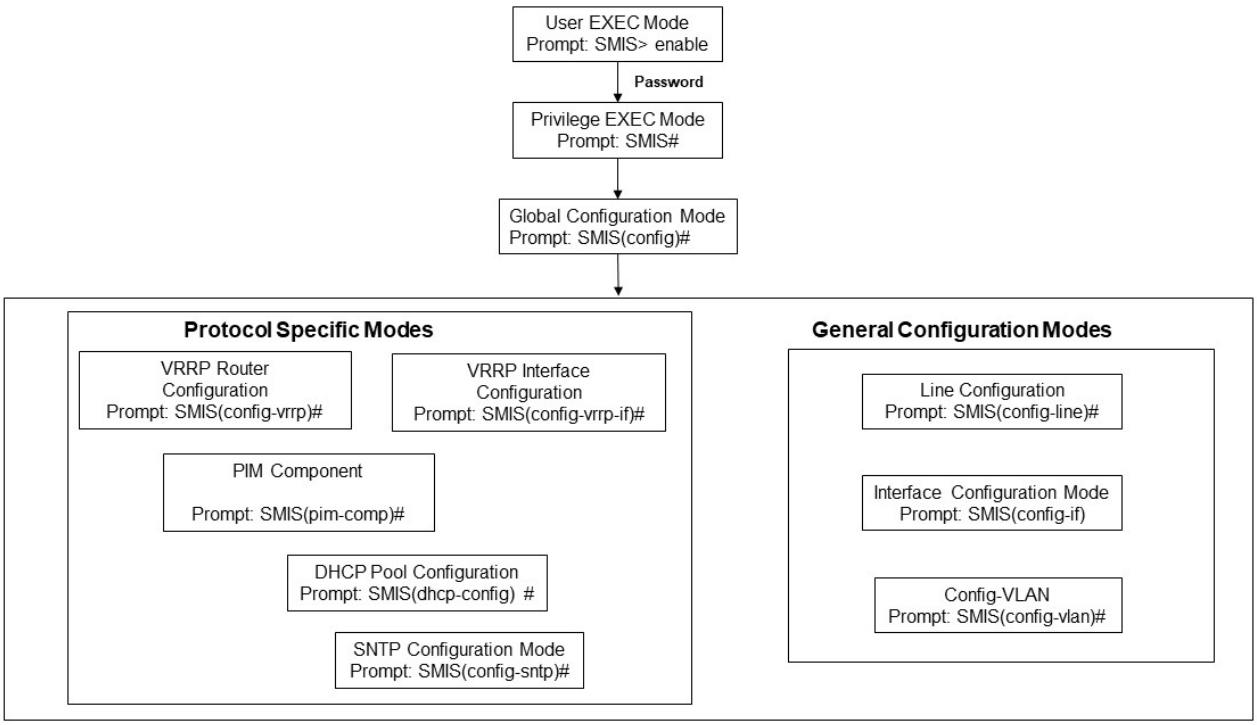
To return to the global configuration mode the **`exit`** command is used.

CEE-Map Configuration Mode

The CEE-Maps described the relationship between traffic priorities and priority-groups, and defined the settings of Priority-based Flow Control (PFC), and bandwidth allocation, to meet the requirement of Data Center Bridging (DCB), conform to the CEE version.

The CEE-Maps will be associated with ports. If a port assocated with a particular CEE-Map, then the port is ready to start a DCBX negotiation with its link partner, to achieve a converged Ethernet channel.

Global configuration mode command **`cee-map <cee-map-id>`** is used to create/enter the CEE-Map to change its settings, the **`exit`** command is used to return to the Global configuration mode. No form of this command to delete the CEE-Map.



3 System Commands

The System Commands describes the commands used to manage access permissions, mode access and terminal configurations on ISS.

The list of CLI commands for the configuration of System commands is as follows:

- Help
- clear screen
- Enable
- Disable
- configure terminal
- configure
- run script
- listuser
- lock
- username
- enable password
- Line
- alias - replacement string
- alias - interface | exec | configure
- access-list provision mode
- access-list commit
- exec-timeout
- logout
- End
- Exit
- show privilege
- show line
- show aliases
- show users
- show history
- password validate char
- password validate uppercase
- password validate lowercase
- password validate numbers
- password validate symbols
- set minimum password length
- show password validate rules
- show minimum password length
- password max-life-time
- show password max-life-time

- `set cli pagination`
- `Coredump`
- `show tech-support`
- `show meminfo`

3.1 help

Command Objective	This command displays a brief description for the given command. To display help description for commands with more than one word, do not provide any space between the words.
Syntax	`help [ command ]`
Mode	All Modes

Example	`Your Product# help enable`
	
	Configure Terminal command must be executed as
	
	`enable [<0-15> Enable Level]`
	
	`[Desc]: Turn on privileged commands.`

3.2 clear screen

Command Objective	This command clears all the contents from the screen.
Syntax	`clear screen`
Mode	All Modes
Example	`Your Product# clear screen`

3.3 enable

Command Objective This command enters into default level privileged mode.

If required, the user can specify the privilege level by enabling level with a password (login password) protection to avoid unauthorized user.

If AAA authorization is enabled, The parameter of privilege doesn't work and the user only could get the privilege from AAA authorization server.

If AAA authorization server downs or doesn't reply, it allows the user fallback the privilege from local account when user enable AAA authorization fallback local otherwise it will set the privilege as 1.

If AAA authorization server reply authorization failed, it will set the privilege as 1.

Syntax `enable [<0-15> Enable Level]`

Parameter Description

- `<0-15> Enable level` - Sets the priviledge level to enter the system.

  This value ranges between 0 and 15– Users with Privilege Level 0 can access only the following commands:

  - enable
  - disable
  - Exit
  - help
  - logout

  This is the most restricted level.

  – Users with Privilege Level 1 can access all user-level commands with SMIS> prompt.

- System allows configuring additional privilege levels (from level 2 to 14) to meet the needs of the users while protecting the system from unauthorized access.
- Users with Privilege Level 15 can access all commands. It is the least restricted level.

Mode	User EXEC Mode
Default	Enable level - 15
Example	`Your Product# enable 15`
Related Command(s)	• **`disable`** –Turns off privileged commands • **`enable password`** – Modifies enable password parameters • **`aaa authorization`** – Enable AAA authorization

3.4 disable

Command Objective	This command turns off privileged commands. This value ranges between 0 and 15. This value should be lesser than the privilege level value given in the enable command.
Syntax	`disable [<0-15> Privilege level to go to]`
Mode	User EXEC Mode
Example	`Your Product# disable 1`
Related Command(s)	• `enable` – Enters to privileged EXEC mode.

3.5 configure terminal

Command Objective	This command enters to Global Configuration Mode which allows the user to execute all the commands that supports global configuration mode.
Syntax	`configure terminal`
Mode	Privileged EXEC Mode
Example	`Your Product# configure terminal` `Your Product (config)#`
Related Command(s)	• **`end`** – Exits from Configuration mode and enters Privilidged Configuration mode • **`exit`** – Exits the current mode and reverts to the mode used prior to the current mode

3.6 configure

Command Objective	This command enters the configuration mode. Configuration from memory or network is not supported, when entered into the configuration mode using this command
	This command is a complete standardized implementation of the existing command and operates similar to that of the command configure terminal
Syntax	`configure`
Mode	Privileged EXEC Mode
Example	`Your Product# configure`
Related Command(s)	• **`end`** – Exits from Current mode and enters Privilidged EXEC mode • **`exit`** - Exits the current mode and reverts to the mode used prior to the current mode.

3.7 run script

Command Objective	This command runs CLI commands from the specified script file.
Syntax	`run script [flash: | slot0: | volatile:] <script file> [<output file>]`
Parameter Description	• `flash: | slot0: | volatile:` - Specifies the source of the script file. – `flash` - The script file is read from the Flash memory. – `slot0` - The script file is read from the PCMCIA card or CompactFlash memory. – This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported – `volatile` - The script file is read from the volatile memory. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported. • `<script file>` - Specifies the script file to be executed • `<output file>` - Specifies the output file
Mode	Privileged EXEC Mode.
Example	`Your Product# run script flash sample.js`

3.8 listuser

Command Objective	This command lists all the default and newly created users, along with their permissible mode.
Syntax	`listuser`
Mode	Privileged EXEC Mode

Example	`Your Product# listuser`
	`USER MODE PRIVILEGE`
	`ADMIN (Admin user) / 15`

Related Command(s)	• `show users` – Displays information about terminal lines

3.9 lock

Command Objective	This command locks the CLI console. It allows the user/system administrator to lock the console to prevent unauthorized users from gaining access to the CLI command shell. Enter the login password to release the console lock and access the CLI command shell.
Syntax	`lock`
Mode	Privileged EXEC Mode
Example	`Your Product# lock`

3.10 username

Command Objective This command creates a user and sets the enable password for that user with the privilege level.

The no form of the command deletes a user and disables the enable password for that user.

If AAA authorization is enabled, it will allow the user have the administrator privilege (15) to use this command. Otherwise, it only allows the administrator user to use this command.

Syntax

```
username <user-name> [password <passwd>] [privilege
<1-15>] [confirm-password <passwd>] [admin]
no username < user-name >
```

Parameter

Description

- `<user-name>` - Specifies the login user name to be created
- `password <passwd>` - Specifies the password to be entered by the user to login to the system, and password encryption to be used. The size password entered must be a minimum of 8 and maximumof 20 characters containing atleast one uppercase, one lowercase, one number and one special character.
- `privilege <1-15>` - Applies restriction to the user for accessing the CLI commands. This values ranges between 1 and 15. For Example, a user ID configured with privilege level as four can access only the commands having privilege ID lesser than or equal to four.
- `confirm-password <passwd>` - Enter the password again to confirm it.
- `admin` - Set the user ID as the admin user.

Mode Global Configuration Mode

☞ Privilege ID is set as zero for all the show commands and is set as 15 for all the configuration commands, in the def files. That is, root users can access all the commands and other users can access only the show commands. Users can change the privilege IDs of the commands in the def file to customize and segregate the commands as per the needs.

If the user "ADMIN" is created as admin user, the password policy is skiped for checking.

If the switch is reset to factory default, the user “ADMIN” is restored and the default password is the unique password printed on the label with the switch serial number and MAC address.

If user already exists, the administrator can re-assign password, privilege and admin for user.

Example

```
Your Product (config)# username products password
Prod@1234 privilege 15 confirm-password Prod@1234
```

The user products is created with the privilege level 15. Hence, the user will be visible to view all the commands.

```
Your Product (config)# username support admin
```

The user support is created with the the privilege level 15 and the default password “Smci123#”. If not an admin user, the user support is created with priviledge level is 1 and the default password

```
Your Product (config)# username support password
Supp@123 privilege 1 confirm-password Supp@123
```

The user support is created with the privilege level 1. Hence, the user will be visible to view only the below commands:

- Show - Show commands related to all the features.
- Enable - Enables the privilege level.
- Disable - Disables the privilege level.
- Exit
- Logout
- Clear
- Debug
- No Debug

Related Command(s)

- `enable password` – Modifies enable password parameters
- `enable` – Enters to privileged EXEC mode
- `lisuser` – Lists all the users
- `aaa authorization` – Enable AAA authorization

3.11 enable password

Command Objective This command modifies enable password parameters.

The no form of the command disables enable password parameters.

Syntax

```
enable password [level (1-15)] <LINE 'enable' password>
no enable password [level (1-15)]
```

Parameter Description

- `level(1-15)` - Represents the privilege level for which the password is to be set. The level ranges from 1 to 15.
- `<LINE 'enable' password>` - Represents the password to be given. Password should follow password configuration conventions where it should contain atleast one uppercase, one lowercase, one number and one special character.

Mode Global Configuration Mode

Example

```
Your Product (config)# enable password level 1 Ad@123
```

Related Command(s)

- `username` – Creates a user and sets the password for that user with the privilege level
- `enable` – Enters to privileged EXEC mode

3.12 line

Command Objective	This command identifies a specific line for configuration and enters the line configuration mode and allows the user to execute all the commands that supports line configuration mode.
Syntax	`line {console | vty | <line-number(0-16)>}[<ending-line- number(3-16)>]`
Parameter Description	• `console` - Specifies the line for configuration as console and enters the console line configuration mode • `vty` - Specifies the line for configuration as Virtual terminal line • `<line-number(0-16)>` - Specifies the ID of a specific telnet session or initial telnet session in a configured series of telnet sessions. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported • `<ending-line-number(3-16)>` - Specifies the ID of the last telnet session in a configured series of telnet sessions. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported
Mode	Global Configuration Mode
Example	`Your Product (config)# line console` `Your Product (config-line)#`
Related Command(s)	• `end` – Exits from Configuration mode and enters Privileged Exec mode • `exit` – Exits the current mode and reverts to the mode used prior to the current mode

- `show line` – TTY line information

3.13 alias - replacement string

Command Objective This command replaces the given token by the given string.

The no form of the command removes the alias created for the given string.

Syntax

```
alias <replacement string> <token to be replaced>

no alias <alias>
```

Parameter Description

- `<replacement string>/ <alias>` - Specifies the string for which a replacement is needed.
- `<token to be replaced>` - Specifies an abbreviated/ short form of the replacement string

Mode Global Configuration Mode

Example

```
Your Product# alias products pdt
```

Related Command(s)

- `show aliases` – Displays the aliases

3.14 alias – interface | exec | configure

Command Objective This command replaces the given token / command with the given string.

This command is a standardized implementation of the existing command. It operates similar to that of the command alias-replacement, except that it allows the user to type a command with multiple tokens without quotes.

Syntax

```
alias {interface | exec | configure} <alias-name>
{command <max 10 tokens> | token }
```

Parameter

Description

- `interface` - Specifies the commands executed in interface configuration mode. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
- `exec` - Specifies the commands executed in privileged EXEC / user EXEC mode. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported
- `configure` - Specifies the commands executed in configuration mode (That is, global, line, profile, vlan, switch and protocol specific configuration modes). This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported
- `<alias-name>` - Specifies the alternate name to be used for the command or token.
- `command <max 10 tokens>` - Specifies the command and token values for which alias name should be configured.
- `token` - Specifies the token for which alias name should be configured.

Mode Global Configuration Mode

☞ Alias name can be set only for the commands having equal to or less than 10 tokens.

Example

```
Your Product (config)# alias ln line
```

Related Command(s)

- `show aliases` - Displays the aliases

3.15 access-list provision mode

Command Objective	This command removes the limit on number of unicast MAC entries indications to control.
Syntax	`access-list provision mode { consolidated | immediate }`
Parameter	
Description	• `consolidated` - Configurates the provision mode as consolidated. • `immediate` - Configurates the provision mode as immediate.
Mode	Global Configuration Mode
Default	immediate
Example	`Your Product (config)# access-list provision mode consolidated`

3.16 access-list commit

Command Objective	This command triggers provisioning of active filter rules to hardware based on configured priority. This command is applicable only when provision mode is consolidated. Traffic flow would be impacted when filter-rules are reprogrammed to hardware.
Syntax	`access-list commit`
Mode	Global Configuration Mode
Example	`Your Product# access-list commit`

3.17 exec-timeout

Command Objective	This command sets a time (in seconds) for EXEC line disconnection. This value ranges between 1 and 18000 seconds. The no form of this command resets the EXEC timeout to its default value.

Syntax	`exec-timeout <integer (1-18000)>`
	
	`no exec-timeout`

Mode	Line Configuration Mode
Default	integer - 1800 seconds
Example	`Your Product (config-line)# exec-timeout 100`
Related Command(s)	• `line` – Configures a console/virtual terminal line

3.18 logout

Command Objective	This command exits from Privileged EXEC/ User EXEC mode to ISS Login Prompt in case of console session. In case of a telnet session, this command terminates the session.
Syntax	`logout`
Mode	User EXEC Mode
Example	`Your Product# logout` `Your Product login:`

3.19 end

Command Objective	This command exits from the current mode to the Privileged EXEC mode.
Syntax	`end`
Mode	All modes
Example	`Your Product# end`
Related Command(s)	• `exit` – Exits the current mode and reverts to the mode used prior to the current mode.

3.20 Exit

Command Objective	This command exits the current mode and reverts to the mode used prior to the current mode
Syntax	`exit`
Mode	All modes
Example	`Your Product# exit`
Related Command(s)	• `end` – Exits from Configuration mode to the Privileged EXEC mode

3.21 show privilege

Command Objective	This command shows the current user privilege level.
Syntax	`show privilege`
Mode	Privileged EXEC Mode
Example	`Your Product# show privilege` `Current privilege level is 15`
Related Command(s)	• `enable` – Enters to Privileged EXEC Mode.

3.22 show line

Command Objective	This command displays TTY line information such as EXEC timeout.
Syntax	`show line {console | vty <line>}`
Mode	Privileged EXEC Mode
Example	`Your Product# show line console` `Current Session Timeout (in secs) = 1800`
Related Command(s)	• `line` – Configures a console/virtual terminal line • `exec-timeout` – Sets a time (in seconds) for EXEC line disconnection. • `clear line vty` – Clears the console or virtual terminal line to an idle state

3.23 show aliases

Command Objective	This command displays all the aliases.
Syntax	`show aliases`

Example	`Your Product# show aliases`
	`show -> sh`
	`privilege -> pr`

Related Command(s)	• `alias-replacement string` – Replaces the given token by the given string.

3.24 show users

Command Objective	This command displays the information about the current user.
Syntax	`show users`
Mode	Privileged EXEC Mode

Example

```
Your Product# show users
Line            User            Peer-Address
0 con           ADMIN            Local Peer
```

Related Command(s)

- `listuse`

– Lists all valid users, along with their permissible mode

3.25 show history

Command Objective	This command displays a list of recently executed commands.
Syntax	`show history`
Mode	Privileged EXEC Mode

Example	`Your Product# show history`
	`1 show ip int`
	`2 show debug-logging`
	`3 show users`
	`4 show line`
	`5 show line console`
	`6 c s`
	`7 show aliases`
	`8 show privilege`
	`9 listuser`
	`10 show users`
	`11 show history`

3.26 password validate char

Command Objective	This command configures the type of characters to be considered for password validation rules and takes values as bit mask. The cli configures the rules for a non-administrator user password.
Syntax	`password validate char [lowercase] [uppercase] [numbers] [symbols]`
Parameter Description	• `lowercase` - Sets lowercase flag for password validation. • `uppercase` - Sets uppercase flag for password validation. • `numbers` - Sets numbers flag for password validation. • `symbols` - Sets symbols flag for password validation.
Mode	Global Configuration Mode
Default	All flags are enabled
Example	`Your Product (config)# password validate char lowercase`
Related Command(s)	• `show password validate rules` - Displays the password validation rules.

3.27 password validate uppercase

Command Objective	This command configures the minimum number of upper case characters that are to be present in the password. If the given password has less than the configured number of upper-case characters, it will not be allowed. This value ranges between 0 and 20.
Syntax	`password validate uppercase [<count(0-20)>]`
Mode	Global Configuration Mode
Default Value	1
Example	`Your Product (config) # password validate uppercase 1`
Related Command(s)	• `show password validate rules` - Displays the password validation rules.

3.28 password validate lowercase

Command Objective	This command configures the minimum number of lower case characters that are to be present in the password. If the given password has less than the configured number of lower case characters, it will not be allowed. This value ranges between 0 and 20.
Syntax	`password validate lowercase [<count(0-20)>]`
Mode	Global Configuration Mode
Default Value	1
Example	`Your Product (config) # password validate lowercase 1`
Related Command(s)	• `show password validate rules` - Displays the password validation rules.

3.29 password validate numbers

Command Objective	This command configures the minimum numerical characters to be present in the password. If the given password has less than the configured number of numerical characters, it will not be allowed This value ranges between 0 and 20.
Syntax	`password validate numbers [<count(0-20)>]`
Mode	Global Configuration Mode
Default Value	1
Example	`Your Product (config) # password validate numbers 1`
Related Command(s)	• `show password validate rules` - Displays the password validation rules.

3.30 password validate symbols

Command Objective	This command configures the minimum special characters to be present in the password. If the given password has less than the configured number of symbols, it will not be allowed. This value ranges between 0 and 20. The following special characters " ' ? : are not accepted as part of the password. The user can use double quotation marks " " to specify a password with special characters, such as "Special 123#".
Syntax	`password validate symbols [<count(0-20)>]`
Mode	Global Configuration Mode
Default Value	1
Example	`Your Product (config) # password validate symbols 1`
Related Command(s)	• `show password validate rules` - Displays the password validation rules.

3.31 set minimum password length

Command Objective	This command configures minimum password length. If the given password has less than the configured password length, it will not be allowed. Maximum password length: 64 characters Minimum password length: 5 characters (default) The cli configures the rules for a non-administrator user password.
Syntax	`set minimum password length <minimum-len>`
Mode	Global Configuration Mode
Default	8
Example	`Your Product (config) # set minimum password length 8`
Related Command(s)	• `show minimum password length` - Displays minimum password length

3.32 show password validate rules

Command Objective This command displays the password validation rules.

Syntax `show password validate rules`

Mode Privileged EXEC Mode

Example

```
Your Product# show password validate rules
 Password Validation Mask : a
 Min Lowercase char count : 2
 Min Uppercase char count : 2
 Min Numeric char count   : 2
 Min Symbol char count    : 2
```

Related Command(s)

- `password validate uppercase` - Sets the minimum uppercase characters to be present in the password
- `password validate lowercase` - Sets the minimum lowercase characters to be present in the password
- `password validate numbers` - Sets the minimum numerical characters to be present in the password
- `password validate symbols` - Sets the minimum special character to be present in the password

3.33 show minimum password length

Command Objective	This command displays minimum password length.
Syntax	`show minimum password length`
Mode	Privileged EXEC Mode
Example	`Your Product# show minimum password length` `Minimum Password length: 8`
Related Command(s)	• `set minimum password length` - Configures minimum password length

3.34 password max-life-time

Command Objective	This command configures the time after which the user password has to be expired in days. This value ranges between 0 and 366 days. The default value of password-max-life-time is 0 days, indicates the password does not expire.
Syntax	`password max-life-time [<days (0-366)>]`
Mode	Global Configuration Mode
Default Value	0 days
Example	`Your Product (config) # password max-life-time 1`
Related Command(s)	• `show password max-life-time` - Displays the password expiry time

3.35 show password max-life-time

Command Objective	This command displays the password expiry time.
Syntax	`show password max-life-time`
Mode	Priviledged EXEC Mode
Example	`Your Product# show password max-life-time` `Password Max Life Time: 365`
Related Command(s)	• `password max-life-time` - Configures the max life time after which the password has to be expired

3.36 set cli pagination

Command Objective	This command enables/disables pagination.
Syntax	`set cli pagination {on | off}`
Mode	Global Configuration Mod

Example	`Your Product(config)# set cli pagination off`
	
	`Your Product(config)#`

Related Command(s)	• Any command which will display long content on the screen, with pagination enabled, the `--More--` prompt will appear and pause listing when certain lines are displayed, users can press any key to resume listing of the content.

3.37 coredump

Command Objective Copies coredump to usb flash disk or remote location.

Syntax coredump {tftp://ip-address/filename | sftp://<user-name>:<pass-word>@ip-address/filename | usb:filename }

Parameter Description

- tftp://ip-address/filename - Configures the TFTP details for taking back up of system logs in TFTP server.
  - ip-address - the IP address or host name of the TFTP server.
  - filename - The name of the file in which the system logs should be stored. Filenames and directory names are case sensitive
- sftp://<user-name>:<pass-word>@ip-address/filename - Configures the SFTP details for taking back up of system logs in SFTP server.
  - user-name - The user name of remote host or server.
  - pass-word – The password for the corresponding user name of remote host or server.
  - ip-address - The IP address or host name of the server.
  - filename - The name of the file in which the system logs should be stored. Filenames and directory names are case sensitive

Mode All Modes

Example `Your Product# coredump tftp://10.0.0.10/test`

3.38 show tech-support

Command Objective	Displays details useful for technical support troubleshooting.
Syntax	`show tech-support`
Mode	All Modes
Example	`Your Product# show tech-support`

3.39 show meminfo

Command Objective	Displays memory information.
Syntax	`show meminfo`
Mode	All Modes
Example	`Your Product# show meminfo`

3.40 set boot

Command Objective	This command configures switch firmware boot up area.
Syntax	`set boot { normal | fallback }`
Mode	Interface Configuration Mode
Default	normal
☞	• This configuration will be reset to default when user execute reset-to-factory-default command.
Example	`Your Product(config-if)# set boot fallback`

Related Command(s)

- `show boot` - Displays current switch firmware boot up area
- `reset-to-factory-default` – Reset configuration to factory default

3.41 show boot

Command Objective	This command is to show current switch firmware boot up area.
Syntax	`show boot`
Mode	Privileged EXEC Mode
☞	• This configuration will be reset to default when user execute reset-to-factory-default command.
Example	`Your Product# show boot`

Related Command(s)

- `set boot` – Configures switch firmware boot up area
- `reset-to-factory-default` – Reset configuration to factory default

3.42 reset-factory-default

Command Objective	This command is to do reset factory default on switch.
Syntax	`reset factory-default`
Mode	Interface Configuration Mode
☞	• This command is to reset to factory default and then reload switch automatically. User must use default password to login into switch after switch rebooting.
Example	`Your Product(config-if)# reset-factory-default`

4 System Features

SMIS offers a rich set of system features to a user, such as login services, copying / writing facilities, duplex / negotiation support, and many other capabilities. Some features have special hardware requirements and others have special design considerations.

CFA (Common Forwarding Agent) is a proprietary module, which acts as a common forwarder of packets between the Network Protocol Module(s), the Data-Link Layer Protocol Layer Module(s) and the Device Drivers. CFA provides central management of the generic parameters of all the interfaces in the system.

The list of CLI commands for the configuration of system features is as follows:

- default mode
- default restore-file
- ip address
- Switchport
- ip address - rarp/dhcp
- login authentication
- login authentication-default
- authorized-manager ip-source
- ip http port
- set ip http
- mtu frame size
- system mtu
- bridge port-type
- system-specific port-id
- set custom-param
- mac- addr
- snmp trap link-status
- Write
- Copy
- copy startup-config
- copy running-config startup –config
- copy logs
- firmware upgrade
- copy – file
- clock set
- erase

- cli console
- flowcontrol
- tunnel mode
- tunnel checksum
- tunnel path-mtu- discovery
- tunnel udlr
- shutdown - physical/VLAN/port-channel/tunnel Interface
- debug interface
- debug-logging
- incremental- save
- auto-save trigger
- set switch maximum – threshold
- set switch temperature – threshold
- set switch power – threshold
- mac-learn-rate
- system contact
- system location
- clear interfaces – counters
- clear counters
- show ip interface
- show authorized-managers
- show interfaces
- show interfaces – counters
- show system-specific port- id
- show custom- param
- show interface mtu
- show interface bridge port-type
- show env
- show system information
- show flow-control
- show debug-logging
- show debugging
- show clock
- show running-config
- show http server status
- show system acknowledgement
- show mac-learn-rate

- port-isolation in_vlan_ID
- show port-isolation
- private-vlan mapping
- audit-logging
- audit-logging filename
- audit-logging filesize
- audit-logging reset show config log
- hol blocking prevention
- internal-lan
- show internal-lan
- show iftype protocol deny table
- clear line vty
- tunnel hop-limit
- login block -for
- audit-logging logsize-threshold
- feature telnet
- show telnet server
- show audit
- set http authentication-scheme
- set http redirection enable
- http redirect
- show http authentication-scheme
- show http redirection
- ENTITY MIB
    - set entity physical-index
    - show entity logical
    - show entity physical
    - show entity lp-mapping
    - show entity alias-mapping
    - show entity phy- containment
- set hitless-restart enable
- speed
- automatic-port-create
- port-type providerInstancePort
- sleep
- rate-limit pause
- cpu controlled learning
- traffic -separation control

- mdix auto
- set port
- config-restore
- set switch-name
- packet receive index
- packet send index port
- packet send index value
- show packet send index
- show packet receive index
- set mirroring
- default exec-timeout
- ip unnumbered
- clear http server statistics
- show license
- install license
- uninstall license
- copy debug-files
- multiplex
- ip mtu frame size
- aaa authentication login ascii-authentication
- aaa authentication login default group
- aaa group server tacacs+
- server

4.1 default mode

Command Objective

This command configures the mode by which the default interface gets its IP address.

This configuration takes effect only on switch restart.

Syntax `default mode { manual | dynamic }`

Parameter Description

- `manual` - Assigns static IP address to the default interface. The IP address and IP mask configured by user are assigned to the default interface.
- `dynamic` - Assigns dynamic IP address to the default interface. That is, IP address provided by the server in the network is assigned to the default interface on switch reboot. The IP address is fetched through the dynamic IP address configuration protocols such as DHCP client, RARP client, and BOOTP client.

Mode Global Configuration Mode

Default manual

Example `Your Product(config)# default mode dynamic`

Related Command(s)

- `show nvram`- Displays the current information stored in the NVRAM

- **`default ip address allocation protocol`** - Configures the protocol by which the default interface acquires its IP address

- **`default ip address`** - Configures the IP address and subnet mask for the default interface.

- **`ip address –rarp/dhcp`** - Configures the current VLAN / OOB interface to dynamically acquire an IP address from the RARP / DHCP server. The no form of the command resets the IP address for the interface to its default value.

4.2 default restore-file

Command Objective	This command configures the path of the default restoration file from which the configuration should be restored in the flash when the system is restarted.
Syntax	`default restore-file <filename>`
Mode	Global Configuration Mode
Default	smis.conf
Example	`Your Product(config)# default restore-file restore.conf`
Related Command(s)	• `show nvram` - Displays the current information stored in the NVRAM

4.3 ip address

Command Objective This command sets the IP address for an interface.

The no form of the command resets the IP address of the interface to its default value.

Syntax

```
ip address <ip-address> <subnet-mask> [secondary]
no ip address [<ip_addr>]
```

Parameter Description

- **<ip-address>** - Sets the IP address for an interface. If the network in which the switch is implemented contains a server such as DHCP server,

  dynamically allocating IP address, the configured IP address should not be within the range of the addresses that will be allocated by the server to the other switches. This precaution avoids creation of IP address conflicts between the switches.

- **<subnet-mask>** - Sets the subnet mask for the configured IP address.

  The configured subnet mask should be in the same subnet of the network in which the switch is placed.

  ✎ The parameters ip-address and subnet-mask are used implicitly in BCM Target.

- **secondary** - Sets the configured IP address as an additional IP address for the interface (that is, the configured address is used as secondary address instead of primary address). The configuration of this feature is not supported on management interface.

Mode Interface Configuration Mode

This command is applicable in VLAN Interface Mode / OOB Interface Mode.

Default

- IP address specified in nvram is taken as default for the default VLAN identifier.
- IP address is assigned as 0.0.0.0 and subnet mask as 255.255.255.255 for other interfaces.

- The interface should be shutdown before executing this command.
- If the IP address of the interface to which you are connected is modified, then the connection to the switch will be lost.

Example

```
Your Product(config-if)# ip address 10.0.0.3
255.255.255.0 secondary
```

Related Command(s)

- `show nvram` - Displays the current information stored in the NVRAM.
- `show ip interface` - Displays the IP interface configuration for all interfaces available in the switch.
- `shutdown – physical/VLAN/port-channel/tunnel Interface` - Disables a physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface.

4.4 switchport

Command Objective This command configures the port as switch port. Only switch port Related Command are made available for the interface, when the port is configured as switch port.

The no form of the command resets the port as router port. Only router port Related Command are made available for the interface, when the port is configured as router port.

Syntax

`switchport`

`no switchport`

Mode Interface Configuration Mode

Default switchport

☞ The interface should be shutdown before executing this command.

Example

```
Your Product(config-if)# switchport
```

Related Command(s)

- `release` - Releases, on the specified interface, the DHCP lease obtained for an IP address from a DHCP server.
- `renew` - Renews the DHCP lease for the interface specified.
- `ip dhcp relay circuit-id` – Configures circuit ID value for an interface.
- `ip dhcp relay remote-id` – Configures remote ID value for an interface.
- `show ip interface` - Displays the IP interface configuration for all interfaces available in the switch.

- switchport filtering-utility-criteria - Creates filtering utility criteria for the port.
- switchport pvid - Configures the PVID on the specified port.
- switchport acceptable-frame-type - Configures the type of VLAN dependant BPDU frames such as GMRP BPDU, that the port should accept during the VLAN membership configuration.
- switchport ingress-filter - Enables ingress filtering feature on the port.
- switchport map protocols-group - Maps the configured protocol group to a particular VLAN ID for an interface.
- switchport priority default - Configures the default ingress user priority for a port.
- switchport mode - Configures the mode of operation for a switch port.
- switchport protected - Enables switchport protection feature for a port.

4.5 ip address - rarp/dhcp

Command Objective This command configures the current VLAN / OOB interface to dynamically acquire an IP address from the RARP / DHCP server.

The no form of the command resets the IP address for the interface to its default value.

Syntax

```
ip address { dhcp | rarp}[client-id { FastEthernet |
GigabitEthernet | Port-channel | Vlan }
<interface_list>] [hostname <host_name>]

no ip address
```

Parameter Description

- `dhcp` - Allows the client device to obtain configuration parameters such as

  network address, from the DHCP server.
- `rarp` - Allows the client device to dynamically find its IP address from

  RARP server, when it has only its hardware address such as MAC address.
- `client-id` - Sets the client identifier that specifies the interface type and hexadecimal MAC address of the specified interface. The various interface types that can be specified are:
  - FastEthernet - Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto

    100 Megabits per second.
  - GigabitEthernet - A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - Port-channel - Logical interface that represents an aggregator which contains several ports aggregated together.

– Vlan - Logical interface that specifies a group of hosts which can communicate with each other as in same broadcast domain.

- <interface list> - Sets the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel and

  VLAN. Only VLAN or port-channel ID is provided, for interface types VLAN and port-channel. Use comma as a separator without space while configuring listof interfaces. Example: 0/1,0/3 or 1,3.

  Feature not supported - This featurehas been included to adhere to the

  Industry Standard CLI syntax. This feature is currently not supported.

- hostname - Sets the name of the host from which the IP address is to be acquired dynamically. Feature not supported - This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode	Interface Configuration Mode (VLAN)
Default	dhcp
Example	`Your Product(config-if)# ip address dhcp`
Related Command(s)	• show ip dhcp client stats - Displays the DHCP client statistics information for interfaces that are configured to acquire IP address dynamically from the DHCP server. • release - Releases, on the specified interface, the DHCP lease obtained for an IP address from a DHCP server. • renew - Renews the DHCP lease for the interface specified

4.6 login authentication

Command Objective This command configures the authentication method for user logins for accessing the GUI to manage the switch. Few network routers and other network equipment allows access to a server or a managing computer to determine if the user attempting to log in has the proper rights or is in the user database.

The no form of the command resets the authentication method for user logins to its default values. Changing login authentication from default to another value may disconnect the telnet session.

Syntax

```
login authentication [{radius | tacacs }] [local]

no login authentication
```

Parameter Description

- **radius** - Sets the RADIUS server to be used as an authentication server. Enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.
- **tacacs** - Sets the TACACS server to be used as an authentication server. Communicates with the authentication server commonly used in networks.
- **local** - Sets locals authentication. The user identification, authentication, and authorization method is chosen by the local system administration and does not necessarily comply with any other profiles.

Mode Global Configuration Mode

Default	Local
Example	`Your Product(config)# login authentication radius`
Related Command(s)	• `username` - Creates a user and sets the enable password for that user with the privilege level • `no enable password` - Deletes a user and disables enable password parameters • `show system information` - Displays system information

4.7 login authentication-default

Command Objective	This command configures the authentication method for user logins for accessing the GUI to manage the switch. Few network routers and other network equipment allows access to a server or a managing computer to determine if the user attempting to log in has the proper rights or is in the user database. Changing login authentication from default to another value may disconnect the telnet session. The no form of the command resets the authentication method for user logins to its default values.
✎	This command is a standardized implementation of the existing command. It operates similar to that of the command **login authentication**.

Syntax	`login authentication { default | <list-name> }`
	
	`no login authentication { default | <list-name> }`

Parameter Description	• `default` - Sets the default authentication method for User Logins. • `<list-name>` - Uses the list of user names created with the user name command, for authentication.
✎	This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
Mode	Global Configuration Mode

Example

```
Your Product(config)# login authentication default
```

Related Command(s)

- `username` - Creates a user and sets the enable password for that user with the privilege level
- `no enable password` - Deletes a user and disables enable password parameters
- `show system information` - Displays system information

4.8 authorized-manager ip-source

Command Objective

This command configures an IP authorized manager.

The no form of the command removes manager from authorized managers list.

Syntax

authorized-manager ip-source <ip-address> [{<subnet-mask>

| / <prefix-length(1-32)>}] [interface [interface-type

<0/a-b, 0/c, ...>] [interface-type <0/a-b, 0/c, ...>]]

[<interface-type <a,b or a-b or a,b,c-d...>]] [vlan <a,b

or a-b or a,b,c-d>] [cpu0] [service [snmp] [telnet] [http]

[https] [ssh]]

no authorized-manager ip-source < ip-address > [{<subnet- mask > | / <prefix-length(1-32)>}]

Parameter

Description

- <ip-address> - Sets the network or host address from which the switch is managed. An address 0.0.0.0 indicates 'Any Manager'."
- <subnet-mask> - Sets the subnet mask for the configured IP address. The configured subnet mask should be in the same subnet of the network in which the switch is placed.
- <prefix-length(1-32)> - Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. The value ranges between 1 and 32.
- interface - Configures the network or host address for the specified interface. The details to be provided are:

– **interface-type** - Sets the type of interface. The interface can be:

- qx-ethernet – A version of LAN standard architecture that supports data transfer upto 40 Gigabits per second.
- gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
- extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- fx-ethernet – A version of Ethernet that supports data transfer upto 25 Gigabits per second. This Ethernet supports only full duplex links.
- cx-ethernet – A version of Ethernet that supports data transfer upto 100 Gigabits per second. This Ethernet supports only full duplex links.

– **interface-type <0/a-b, 0/c, ...>** - Sets the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash. Use commaas a separator without space while configuring list of interfaces.\

Example: 0/1,0/3 or 1,3.

- **<interface-type <a,b or a-b or a,b,c-d...>** – Configures the network or host address for the specified port-channel interface. Port-channel is a Logical interface that represents an aggregator which contains several ports aggregated together.Configures the port-channel interface identifier. This is a unique value that represents the specific interface. Only port-channel ID is provided port-channel. For Example: 1 represents port-channel ID. Use comma as a separator without space while configuring list of interfaces. Example: 1, 2, 3 or 1-3.
- **vlan <a,b or a-b or a,b,c-d>** - Sets the list of VLANs or a single specifc VLAN in which the IP authorized manager can reside.
- **cpu0** - Configures the access rights for the manager of the switch through OOB Port.
- **service** - Configures the type of service to be used by the IP authorized manager. The values can be:

- **ssh** - Logs into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist. SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker who has managed to take over a network can only force ssh to disconnect. He or she cannot play back the traffic or hijack the connection when encryption is enabled.

- **http** - Defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For Example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page

- **https** – Transmits data securely over the World Wide Web. S-HTTP is designed to transmit individual messages in a secured manner.

- **snmp** - Manages complex networks. SNMP works by sending messages, called PDUs, to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in MIBs and return this data to the SNMP requesters.

Mode Global Configuration Mode

Default All services are allowed for the configured manager

Example

```
Your Product(config)# authorized-manager ip-source
10.203.113.5 255.255.255.255 interface gigabitethernet 0/1
vlan 1 service snmp
```

Related Command(s)

- **show authorized managers** - Displays the configured authorized managers

4.9 ip http port

Command Objective	This command sets the HTTP port. This port is used to configure the router using the Web interface. The value ranges between 1 and 65535. The no form of the command resets the HTTP port to its default value.

Syntax	`ip http port <port(1-65535)>`
	
	`no ip http port`

Mode	Global Configuration Mode
Default	80
☞	HTTP port number configuration takes effect only when HTTP is disabled and enabled again.
Example	`Your Product(config)# ip http port 90`
Related Command(s)	• `Set ip http` - Enables/disables HTTP • `show http server status` - Displays the http server status

4.10 set ip http

Command Objective	This command enables/disables HTTP in the switch.
Syntax	`set ip http {enable | disable}`
Parameter Description	• `enable` - Enables HTTP in the switch. • `disable` - Disables HTTP in the switch.
Mode	Global Configuration Mode
Default	enable
Example	**Your Product(config)# set ip http disable**
Related Command(s)	• `ip http port` - Sets the HTTP port • `show http server status` - Displays the http server status

4.11 mtu

Command Objective	This command configures the maximum transmission unit frame size for all the frames transmitted and received on all the interfaces in a switch. The size of the MTU frame size can be increased using this command. The value ranges from 46 to 9216. This value defines the largest PDU that can be passed by the interface without any need for fragmentation. This value is shown to the higher interface sub- layer and should not include size of the encapsulation or header added by the interface. This value represents the IP MTU over vlan IP interface (Not include router port) , if IP is operating over the interface.
Syntax	**mtu <frame-size(46-9216)>**
Mode	Interface Configuration Mode (Vlan / Physical/ Port channel)
Default	1500
☞	• This configuration can be done, only if the interface is administratively down. • The MTU value should not be greater than 1500 for fastEthernet interface. • Any messages larger than the MTU are discarded silently by the hardware
Example	**Your Product(config-if)# mtu 900**

Related Command(s)

- `show interfaces` - Displays the interface status and configuration
- `show interface mtu` - Displays the global maximum transmission unit
- `shutdown-physical/VLAN/port-channel/tunnel Interface` – Enables the physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface.

4.12 system mtu

Command Objective	This command configures the maximum transmission unit frame size for all the frames transmitted and received on all the interfaces in a switch. The size of the MTU frame size can be increased using this command. The value ranges between 90 and 9216. The no form of this command sets the maximum transmission unit to the default value in all interfaces. This value defines the largest PDU that can be passed by the interface without any need for fragmentation. This value is shown to the higher interface sub-layer and should not include size of the encapsulation or header added by the interface. This value represents the IP MTU over the interface, if IP is operating over the interface.
✎	This command is a standardized implementation of the existing command. It operates similar to that of the command **mtu frame size**.
Syntax	`system mtu <frame-size(90-9216)>` `no system mtu`
Mode	Global configuration mode
Default	1500
☞	• This configuration can be done, only if the interface is administratively down. • Any messages larger than the MTU are discarded silently by the hardware

Example

```
Your Product(config)# system mtu 200
```

Related Command(s)

- `show interfaces` - Displays the interface status and configuration
- `show interface mtu` - Displays the global maximum transmission unit

4.13 bridge port-type

Command Objective This command configures the bridge port type for an interface. It is not supported but reserved for future release.

Syntax

```
bridge port-type { providerNetworkPort |
customerNetworkPort {port-based | s-tagged | c-
tagged} | customerEdgePort | propCustomerEdgePort |
propCustomerNetworkPort | propProviderNetworkPort |
customerBridgePort | customerBackbonePort}
```

Parameter

Description

- `providerNetworkPort` - Sets the bridge port type as provider network port. This option is applicable in provider bridges and provider backbone b-component bridge modes. The port is connected to a single provider.
- `customerNetworkPort` - Sets the bridge port type as customer network port. It has the following options:
  - `port-based` – Sets the bridge port type as port based.
  - `s-tagged` - – Sets the bridge port type as s-tagged
  - `c-tagged` - – Sets the bridge port type as c-tagged
- `customerEdgePort` - Sets the bridge port type as Customer Edge Port.

  The port is in a PEB that is connected to a single customer. The packets received on this port are initially classified to a CVLAN. CVLAN

  classification is done based on the VID in the C-tag present in the packet or from the PVID of the port. Service instance selection is done for a frame

  based on the entry present in the C-VID registration table for the pair (C- VID, reception port).
- `propCustomerEdgePort` - Sets the bridge port type as Proprietary Customer Edge Port. The port is connected to a

single customer, where multiple services can be provided based on only proprietary SVLAN classification tables. S-VLAN classification is not done based on C-VID registration table on the port.

- **propCustomerNetworkPort** - Sets bridge port type as Proprietary Customer Network Port. The port is connected to a single customer, where multiple service can be provided based on CVLANs by assigning one of the proprietary SVLAN classification tables to the port. The services can also be assigned using other proprietary SVLAN classification tables, where CVLAN is not the index of the table.

- **propProviderNetworkPort** - Sets bridge port type as Proprietary Provider Network Port. The port is connected to a Q-in-Q bridge located inside the provider network. The port acts as a part of S-VLAN component. The packets to be tagged and sent out of the port contain 0x8100 as its ethertype. The packets received with standard Q tag is considered as S- Tagged packets.

- **customerBridgePort** - Sets bridge port type as Customer Bridge Port. The port is to be used in customer bridges and in provider (Q-in-Q) bridges. This port type is not valid in PCBs and PEBs.

- **customerBackbonePort** - Sets bridge port type as Backbone Edge Bridge Port that can receive and transmit I-tagged frames for multiple customers, and assign B-VIDs and translate I-SID on the basis of the received I-SID. CBPs are applicable only on PBB B Components.

Mode Interface Configuration Mode

Default

- providerNetworkPort for provider core and edge bridges.
- customerBridgePort for customer bridges.

☞

- Tunneling must be enabled to change port type from Provider Network Port.
- Tunneling must be disabled to change port type to Provider Network Port.
- Port must be administratively down for changing to another port type.
- Bridge port-type is supported only in the following Bridge Modes:

  Provide Edge Bridge

  – Provider Core Bridge
  – Provider Backbone Bridge I Component
  – Provider Backbone Bridge B Component

- In case of Provider Bridge or Customer Bridge, bridge port type will always be `customerBridgePort.`
- `customerEdgePort` is valid only in Provider Edge Bridge.
- All other port types excluding `customerBridgePort` and `customerEdgePort` are valid in both Provide Edge Bridge and Provider Core Bridge.
- Bridge port type can be set only for switch ports and not for router ports, IVR interfaces and I-LAN interfaces.
- The port type cannot be set for a port-channel port, if physical ports are aggregated in the port-channel.
- The port type cannot be set for a port that is part of a port-channel.

Example

```
Your Product(config-if)# bridge port-
type providerNetworkPort
```

Related Command(s)

- **`show interface bridge port-type`** - Displays the Bridge Port Type of interfaces in the switch

- **`switchport acceptable-frame-type`** - Configures the type of VLAN dependant BPDU frames such as GMRP BPDU, that the port should accept during the VLAN membership configuration.

- **`switchport ingress-filter`** - Enables ingress filtering feature on the port.

- **`tunnel mode`** – Configures the tunnel interface with the associated parameters.

- **`switchport`** - Configures the port as switch port.

4.14 system-specific port-id

Command Objective	This command configures the system specific index for the port. It provides a different numbering space other than the IfIndex to identify ports. The value ranges between 1 and 16384. If no other value has been configured, 0 is set by default.
Syntax	`system-specific port-id <integer (1-16384)>`
Mode	Interface Configuration Mode
Default	0
Example	`Your Product(config-if)# system-specific port-id 50`
Related Command(s)	• `show system-specific port-id` - Displays the custom-param configurations.

4.15 set custom-param

Command Objective	This command configures the custom parameters for a particular port. The no form of the command deletes the custom parameter configurations.

Syntax	`set custom-param {type <integer> length <integer> value <string> | attribute <integer (1-4)> value <integer (0-4294967295)>}`
	
	`no custom-param [type <integer>] [attribute <integer (1-4)>]`

Parameter Description	• `type` - Sets the type of the TLV information. • `length` - Sets the length of the TLV information. • `value` - Sets the value of the TLV information. • `attribute` - Sets the opaque attribute ID configured on the port. The value ranges between 1 and 4. • `value` - Sets the value for the Opaque attribute. The value ranges between 0 and 4294967295.
Mode	Interface Configuration Mode
Default	value - 0

Example

```
Your Product(config-if)# set custom-param attribute 2
value 40
```

Related Command(s)

- `show custom-param` - Displays the custom-param configurations.

4.16 mac-addr

Command Objective	This command configures unicast MAC address for the interface.
Syntax	`mac-addr <aa:aa:aa:aa:aa:aa>`
Mode	Interface Configuration Mode
Default	MAC address of the switch is assigned as MAC address for the interface.
☞	• The MAC address can be set only when ifMainAdminStatus for the interface is down. • The object is valid only for interfaces that have the ifMainType set as ethernetCsmacd(6) or ieee8023ad(161).
Example	`Your Product(config-if)# mac-addr 00:22:33:44:55:66`
Related Command(s)	• `show interfaces` - Displays the interface status and configuration.

4.17 snmp trap link-status

Command Objective This command enables trap generation on the interface. The interface generated linkUp or linkDown trap. The linkUp trap denotes that the communication link is available and ready for traffic flow. The linkDown trap denotes that the communication link failed and is not ready for traffic flow.

The no form of this command disables trap generation on the interface.

Syntax

```
snmp trap link-status

no snmp trap link status
```

Mode Interface Configuration Mode

Default SNMP trap link status is enabled

Example

```
Your Product(config-if)# snmp trap link-status
```

Related Command(s)

- `show interfaces` - Displays the interface status and configuration.

4.18 Write

Command Objective This command writes the running-config to a flash file, startup-configuration file or to a remote site.

Syntax

```
write { flash:filename | startup-config |
tftp://ip- address/filename | sftp://<user-
name>:<pass-word>@ip- address/filename }
```

Parameter

Description

- `flash:filename` - Configures the name of the file to which the configuration is to be saved. This file is present in the flash.
- `startup-config` - Starts the switch with the saved configuration on reboot.
- `tftp` - Configures the TFTP related details for writing the configuration to a file in TFTP server.
  - `ip-address` - The IP address or host name of the server in which configuration should be maintained.
  - `filename` - The name of the file in which the configuration should be written. Filenames and directory names are case sensitive
- `sftp` - Configures the SFTP related details for writing the configuration to a file in SFTP server.
  - `user-name` - The user name of remote host or server.
  - `pass-word` – The password for the corresponding user name of remote host or server
  - `ip-address` - The IP address or host name of the server in which configuration should be maintained.
  - `filename` - The name of the file in which the configuration should be written. Filenames and directory names are case sensitive

Mode	Privileged EXEC Mode
Example	`Your product# write startup-config`
Related Command(s)	• `show nvram` - Displays the current information stored in the NVRAM • `show system information` - Displays system information

4.19 copy

Command Objective This command copies the configuration from a remote site to flash.

Syntax

```
copy { tftp://ip-address/filename startup-config |
sftp://<user-name>:<pass-word>@ip-address/filename
startup- config | flash: filename startup-config |
cust:/filename startup-config}
```

Parameter Description

- **tftp://ip-address/filename startup-config** - Configures the address from which the file is to be copied and the file name from which configuration is to be copied. This option configures the TFTP server details Filenames and directory names are case sensitive
- **sftp://<user-name>:<pass-word>@ip-address/filename** - Configures the name of the file in remote location to be copied (downloaded) into configuration file (smis.conf). This option configures theSFTP server details. Filenames and directory names are case sensitive
- **flash: filename startup-config** - Configures the name of the file in flash. The configuration in the flash file are used. Filenames are case sensitive
- **cust:/filename startup-config** - Configures the name of the file in USB drive. The configuration in the USB flash file are used. Filenames are case sensitive.

Mode Privileged EXEC Mode

Example

```
Your Product# copy flash:clcliser startup-config
```

4.20 copy startup-config

Command Objective This command takes a backup of the initial configuration in flash or at a remote location.

Syntax

```
copy startup-config {flash: filename |
tftp://ip- address/filename | sftp://<user-
name>:<pass-word>@ip- address/filename |
cust:/filename }
```

Parameter Description

- `flash: filename` - Configures the name of the file in which the initial configuration should be stored. This file is available in the Flash.
- `tftp://ip-address/filename` - Configures the TFTP details for taking back up of initial configuration in TFTP server.
  - `ip-address` - The IP address or host name of the server.
  - `filename` - The name of the file in which the initial configuration should be stored. Filenames and directory names are case sensitive
- `sftp://<user-name>:<pass-word>@ip-address/filename` - Configures the SFTP details for taking back up of initial configuration in SFTP server.
  - `user-name` - The user name of remote host or server
  - `pass-word` – The password for the corresponding user name of remote host or server
  - `ip-address` - The IP address or host name of the server
  - `filename` - The name of the file in which the initial configuration should be stored. Filenames and directory names are case sensitive

- `cust:/filename` - Configures the file for taking back up of initial configuration in USB drive.

Mode	Privileged EXEC Mode
Example	`Your product# copy startup-config flash:clcliser`
Related Command(s)	• `copy running-config startup-config` - Copies variables from the running configuration to the startup configuration file in NVRAM • `copy-file` - Copies a file from a source remote site /flash to a destination remote site/flash

4.21 copy running-config startup-config

Command Objective	This command copies the variables from the running configuration to the startup configuration file in NVRAM, where the running-config is the current configuration in the switch and the startup config is the configuration that is loaded when the switch boots up.
✐	This command is a complete standardized implementation of the existing command. It operates similar to that of the command **`copy startup-config`.**
Syntax	`copy running-config startup-config`
Mode	Privileged EXEC Mode
Example	**`Your product# copy running-config startup-config`**
Related Command(s)	• `copy startup-config` - Copies variables from the running configuration to the startup configuration file in NVRAM • `copy-file` - Copies a file from a source remote site /flash to a destination remote site/flash

4.22 copy logs

Command Objective This command writes the in-core (RAM-bufferred) debug logs to a remote site.

Syntax

```
copy logs {tftp://ip-address/filename |
sftp://<user- name>:<pass-word>@ip-
address/filename | usb:filename}
```

Parameter

Description

- `tftp://ip-address/filename` - Configures the TFTP details for taking back up of in-core debug logs in TFTP server.
  - ip-address - the IP address or host name of the TFTP server.
  - filename - The name of the file in which the debug logs should be stored. Filenames and directory names are case sensitive
- `sftp://<user-name>:<pass-word>@ip-address/filename` - Configures the SFTP details for taking back up of in-core debug logs in SFTP server.
  - `user-name` - The user name of remote host or server.
  - `pass-word` – The password for the corresponding user name of remote host or server.
  - `ip-address` - The IP address or host name of the server.
  - `filename` - The name of the file in which the debug logs should be stored. Filenames and directory names are case sensitive
- `usb:filename` – Specify the file name in the USB storage for writing the in-core debug logs.

Mode	All Modes

Example	`Your Product# copy logs tftp://10.0.0.10/clcliser`

4.23 firmware upgrade

Command Objective	This command performs firmware upgrade using TFTP from a remote location.
Syntax	`firmware upgrade {tftp://ip-address/filename} {flash:normal	flash:fallback}`
Parameter	
Description	• `tftp://ip-address/filename` - Configures the file to be used for firmware upgrade and its source URL. – `ip-address` - IP address or host name of the TFTP server – `filename` - The name of the file to be used for firmware upgrade. Filenames and directory names are case sensitive • `flash:normal` - Sets the flash in normal image. • `flash:fallback` - Sets the fallback image in Flash
Mode	Privileged EXEC Mode
☞	In stacking environment case, this command copies the image to the attached peers.
Example	`Your Product# firmware upgrade tftp://12.0.0.100/Ramdisk.bin flash:normal`

4.24 copy - file

Command Objective This command copies a file from a source remote site /flash to a destination remote site/flash. The entire copying process takes several minutes and differs from protocol to protocol and from network to network.

Syntax

copy { tftp://ip-address/filename | sftp://<user-name>:<pass-word>@ip-address/filename | flash:filename | cust:/filename}

{tftp://ip-address/filename | sftp://<user-name>:<pass- word>@ip-address/filename | cust:/filename | flash: filename | filename }

Parameter Description

- **tftp://ip-address/filename** - Configures the TFTP details to / from which file to be copied.
  - **ip-address** - IP address or host name of the TFTP server
  - **filename** - Name of the file to be copied or file to which information is to be copied. Filenames and directory names are case sensitive
- **sftp://<user-name>:<pass-word>@ip-address/filename** - Configures the SFTP details to / from which file to be copied.
  - **user-name** - User name of remote host or server
  - **pass-word** – Password for the corresponding user name of remote host or server
  - **ip-address** - IP address or host name of the server
  - **filename** - Name of the file to be copied or file to which information is to be copied. Filenames and directory names are case sensitive
- **cust:/filename** - Configures the name of the file to be copied. This file is present in USB. Filenames are case sensitive

- **flash: filename** - Configures the name of the file to be copied. This file is present in Flash. Filenames are case sensitive
- **filename -** Configures the name of the file to be copied. Filenames are case sensitive.

Mode	Privileged EXEC Mod
Example	`Your product# copy tftp://12.0.0.2/clclirel flash:clcliser`
Related Commands	• `copy running startup-config` - Copies variables from the running configuration to the startup configuration file in NVRAM • `copy startup-config` - Copies variables from the running configuration to the startup configuration file in NVRAM

4.25 clock set

Command Objective

This command manages the system clock.

Syntax

`clock set hh:mm:ss <day (1-31)>`

`{january|february|march|april|may|june|july|august|september |october|november|december} <year (2000 - 2035)>`

Parameter Description

- `hh:mm:ss` - Sets the current time. The format is hour, minutes and seconds.
  - `<day (1-31)>` - Sets the current day. It ranges between 1 and 31.
  - `january` - Sets the month as January.
  - `february` - Sets the month as February
  - `march` - Sets the month as march
  - `april` - Sets the month as april
  - `may` - Sets the month as may
  - `june` - Sets the month as June
  - `july` - Sets the month as July
  - `august` - Sets the month as August
  - `september` - Sets the month as September
  - `october` - Sets the month as October
  - `november` - Sets the month as November

– `december` - Sets the month as December

– `<year (2000 - 2035)>` - Sets the year. It ranges between 2000 and 2035

Mode	Privileged EXEC Mode
Example	`Your product# clock set 18:04:10 18 Oct 2015`
Related Command(s)	• `show clock` - Displays the system clock

4.26 erase

Command Objective	This command clears the contents of the startup configuration or sets parameters in NVRAM to default values.
Syntax	`erase {startup-config | nvram: | flash:filename}`
Parameter Description	• `startup-config` - Clears the startup configuration file • `nvram` - Clears the content from NVRAM • `flash:filename` - Clears the content from the local system flash file.
Mode	Privileged EXEC Mode
Example	`Your Product# erase startup-config`
Related Command(s)	• `show nvram` - Displays the current information stored in the NVRAM • `show system information`- Displays system information

4.27 cli console

Command Objective	This command enables the console CLI through a serial port. The no form of the command disables console CLI.
Syntax	`cli console` `no cli console`
Mode	Privileged EXEC Mode
Default	Enabled
☞	This command takes effect only on system restart.
Example	`Your Product# cli console`
Related Command(s)	• `show nvram` - Displays the current information stored in the NVRAM.

4.28 flowcontrol

Command Objective This command is used to set the send or receive flow-control value for an interface.

- If flowcontrol send is on for a device and if it detects any congestion at its end, then it notifies the link partner or the remote device of the congestion by sending a pause frame.
- If flowcontrol receive is on for the remote device and it receives a pause frame, then it stops sending any data packets. This prevents any loss of data packets during the congestion period.
- PAUSE is a flow control mechanism that is implied on full duplex Ethernet link segments. The mechanism uses MAC control frames to carry the PAUSE commands.

Interface must first be made administratively down before setting flow control status

Syntax `flowcontrol { send | receive} { on | off | desired}`

Parameter

Description

- `send` - Sets the interface to send flow control packets to a remote device
- `receive` - Sets the interface to receive flow control packets from a remote device
- `on` - If used with receive allows an interface to operate with the attached device to send flow control packets. If used with send the interface sends flowcontrol packets to a remote device if the device supports it

- **off** - Turns-off the attached devices (when used with receive) or the local ports (when used with send) ability to send flow-control packets to an interface or to a remote device respectively
- **desired** - Allows a local port to operate with an attached device that is required to send flow control packets or that may send the control packets, when used with receive option. Allows the local port to send administrative status to a remote device if the remote device supports it, when used with send option.

Mode Interface Configuration Mode

Default The default flow control for the interfaces are

- flowcontrol receive off
- flowcontrol send off

Example

```
Your Product(config-if)# flowcontrol send on
```

Related Command(s)

- **show interfaces** - Displays the interface status and configuration
- **show flow-control** - Displays the flowcontrol information

4.29 tunnel mode

Command Objective

This command configures the tunnel interface with the associated parameters.

This tunnel feature is not supported.

The no form of the command deletes the tunnel interface and its associated parameters.

Syntax

```
tunnel mode {gre|sixToFour|isatap|compat|ipv6ip} [config-id
<ConfId(1-2147483647)>] source <TnlSrcIP/IfName> [dest
<TnlDestIP>]

no tunnel mode {gre|sixToFour|isatap|compat|ipv6ip} [config-id <ConfId(1-2147483647)>] source
<TnlSrcIP/IfName/IfIndex> [dest <TnlDestIP>]
```

Parameter Description

- **gre** - Sets the tunnel in Generic Router Encapsulation mode.
- **sixToFour** - Sets the tunnel in six to four encapsulation mode.
- **isatap** - Sets the tunnel in ISATAP Encapsulation mode.
- **compat** - Sets the tunnel in IPv6 auto compatible encapsulation mode.
- **ipv6ip** - Sets the tunnel in IPv6 over IPv6 configured encapsulation mode.
- **config-id<ConfId(1-2147483647)>** - Sets an identifier to distinguish between multiple tunnels of the same encapsulation method, with same end-points. This value ranges between 1 and 2147483647.

- **source<TnlSrcIP/IfName>** - Sets the local end point address of the tunnel
- **dest<TnlDestIP>** - Sets the remote end point address of the tunnel

Mode	Interface Configuration Mode (Tunnel interface mode)
Example	`Your Product(config-if)# tunnel mode ipv6ip config-id 1 source vlan1 dest 10.203.113.114`
Related Command(s)	• **show interfaces** - Displays the interface status and configuration

4.30 tunnel checksum

Command Objective	This command enables end-to-end check summing of packets. This feature is not supported. The no form of the command disables end-to-end check summing of packets.

Syntax	`tunnel checksum`
	
	`no tunnel checksum`

Mode	Interface Configuration Mode (Tunnel interface mode)
Default	disabled
☞	This command is applicable only for GRE Encapsulation Method.
Example	`Your Product(config-if)# tunnel checksum`
Related Command(s)	• `show interfaces` - Displays the interface status and configuration

4.31 tunnel path-mtu-discovery

Command Objective This command enables Path MTU discovery on Tunnel. It is not supported.

The no form of the command disables Path MTU discovery on Tunnel.

Syntax

```
tunnel path-mtu-discovery [age-timer {<integer (5-254)> | infinite}]

no tunnel path-mtu-discovery
```

Parameter Description

- `<integer (5-254)>` - Configures timeout in minutes, after which the estimate of the PMTU is considered stale. This value ranges between 5 and 254.
- `infinite` - Configures the PMTU timeout as infinite. Does not detect any increase in PMTU.

Mode Interface Configuration Mode (Tunnel interface mode)

Default Disabled

Example

```
Your Product(config-if)# tunnel path-mtu-discovery
age- timer 5
```

Related Command(s)

- `show interfaces` - Displays the interface status and configuration

4.32 tunnel udlr

Command Objective	This command associates tunnel with a unidirectional interface. It is not supported. The no form of the command associates tunnel with a Bidirectional interface.

Syntax	`tunnel udlr {receive-only | send-only}`
	
	`no tunnel udlr`

Parameter **Description**	• `receive-only` - Sets the uni-directional tunnel as incoming only. • `send-only` - Sets the uni-directional tunnel as outgoing only.
Mode	Interface Configuration Mode (Tunnel interface mode)
Example	`Your Product(config-if)# tunnel udlr receive-only`
Related Command(s)	• `show interfaces` - Displays the interface status and configuration

4.33 shutdown - physical/VLAN/port-channel/tunnel Interface

Command Objective	This command disables a physical interface / VLAN interface / port-channel interface / tunnel interface. The no form of the command enables a physical interface / VLAN interface / port-channel interface / tunnel interface.

Syntax	`shutdown`
	
	`no shutdown`

Mode	Interface Configuration Mode for physical interface / port-channel/tunnel interface/OOB Interface VLAN Interface Mode for VLAN interface
Default	• The Management Interface is always enabled • The interface VLAN 1 is enabled • The other interfaces are disabled
☞	• All functions on the specified interface are disabled by the shutdown command
Example	`Your Product(config-if)# shutdown`

Related Command(s)

- `show spanning-tree - Summary, Blockedports, Pathcost, redundancy` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.

- **show spanning-tree detail** - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- **show spanning-tree active** - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- **show spanning-tree – layer 2 gateway port** - Displays spanning tree information for all L2GPs enabled in the switch.
- **show spanning-tree mst - CIST or specified mst Instance** - Displays multiple spanning tree information for all MSTIs in the switch.
- **show interfaces** - Displays the interface status and configuration

4.34 debug interface

Command Objective

This command sets the debug traces for all the interfaces.

The no form of the command resets the configured debug traces.

Syntax

```
debug interface [track] [enetpktdump]
[ippktdump] [arppktdump] [trcerror] [os]
[failall] [buffer] [all]
```

```
no debug interface [track] [enetpktdump]
[ippktdump] [arppktdump] [trcerror] [os]
[failall] [buffer] [all]
```

Parameter Description

- `track` - Generates debug messages for all track messages.
- `enetpktdump` - Generates debug messages for ethernet packet dump messages.
- `ippktdump` - Generates debug messages for IP protocol related packet dump messages.
- `arppktdump` - Generates debug messages for address resolution protocol related packet dump messages.
- `trcerror` - Generates debug messages for trace error messages.
- `os` - Generates debug messages for for OS resources. For Example, when there is a failure in mem pool creation / deletion, this trace level is used
- `failall` - Generates debug messages for all failures including packet validation.
- `buffer` - Generates debug messages for buffer trace levels where packet buffer is used, i.e in cases where packet is enqueued
- `all` - Generates debug messages for all kinds of traces.

Mode

Privilege EXEC mode

Example

```
Your product# debug interface track
```

4.35 debug-logging

Command Objective	This command configures the logging option of debug traces. Debug logs are directed to the console screen, or to the RAM disk file, or to the flash file, which can later be uploaded, based on the input. The no form of the command displays debug logs in the RAM disk file.

Syntax	`debug-logging { console | ram | flash}`
	
	`no debug-logging`

Parameter **Description**	• `console` - Specifies the logging of traces at the console • `ram` - Specifies the logging of traces to a RAM disk file • `flash` - Specifies the logging of traces into a flash file
Mode	Global Configuration Mode
Default	ram
Example	`Your Product(config)# debug-logging console`
Related Command(s)	• `show debug-logging` - Displays the debug logs stored in RAM disk file

4.36 incremental-save

Command Objective	This command enables/disables the incremental save feature.
Syntax	`incremental-save { enable | disable }`
Parameter Description	• `enable` - Enables the incremental save feature. • `disable` - Disables the incremental save feature.
Mode	Global Configuration Mode
Default	enable
Example	`Your Product(config)# incremental-save enable`
Related Command(s)	• `show nvram` - Displays the current information stored in the NVRAM.

4.37 auto-save trigger

Command Objective	This command enables / disables the auto save trigger function.
Syntax	`auto-save trigger { enable | disable }`
Parameter Description	• `enable` - Enables the auto save trigger function. • `disable` - Disables the auto save trigger function.
Mode	Global Configuration Mode
Default	disable
Example	`Your Product(config)# auto-save trigger enable`
Related Command(s)	• `show nvram` - Displays the current information stored in the NVRAM.

4.38 set switch maximum - threshold

Command Objective This command sets the switch maximum threshold values of RAM, CPU, and Flash. When the current resource usage rises above the threshold limit, the SNMP trap message with maximum severity will be sent for the specified resource and the syslog message will be displayed. This threshold value is represented in percentage and ranges between 1 and 100 percentage

Syntax

```
set switch maximum { RAM | CPU | flash } threshold

<percentage (1-100)>
```

Parameter Description

- `RAM` - Indicates the maximum RAM usage of the switch in percentage.

  When the RAM usage crosses the threshold percentage, an SNMP trap with

  maximum severity will be sent to the manager.

- `CPU` - Indicates the maximum CPU usage of the switch in percentage. When CPU load exceeds the threshold value, an SNMP trap with maximum severity will be sent to the manager.

- `flash` - Indicates the maximum flash usage of the switch in percentage.

  When the flash usage crosses the threshold percentage an SNMP trap with maximum severity will be sent to the manager.

- `percentage (1-100)` - Configures the threshold value in percentage.

  This value ranges between 1 and 100 percentage

Mode Global Configuration Mode

Default

- RAM - 100%
- CPU - 100 %

- flash - 100%

Example	`Your Product(config)# set switch maximum RAM threshold 98`
Related Command(s)	• `show env` - Displays the switch related information such as CPU, Flash and RAM usage, and also displays the current power and temperature of the switch

4.39 set switch temperature - threshold

Command Objective	This command sets the maximum and minimum temperature threshold values of the switch in celsius. When the current temperature drops below the threshold, an SNMP trap with maximum severity will be sent to the manager. This threshold value ranges between -14 and 40 degree Celsius.
	This command is a complete standardized implementation of the existing command **`set switch maximum - threshold`**.
Syntax	`set switch temperature {min|max} threshold <celsius (-14 - 40)>}`
Parameter **Description**	• `min -` Sets the minimum temperature threshold value for the switch. When the current temperature drops below the threshold, an SNMP trap with maximum severity will be sent to the manager • `max -` Sets the maximum temperature threshold value for the switch. When the current temperature rises above the threshold, an SNMP trap with maximum severity will be sent to the manager
Mode	Global Configuration Mode
Default	• min - 10 degree Celsius • max - 40 degree Celsius
Example	**`Your Product(config)# set switch temperature min threshold -10`** **`Your Product(config)# set switch temperature max threshold 37`**

Related Command(s)	• `show env` - Displays the switch related information such as CPU, Flash and RAM usage, and also displays the current power and temperature of the switch

4.40 set switch power - threshold

Command Objective	This command sets the maximum and minimum threshold values of the switch power supply in volts. When the current temperature drops below the threshold, an SNMP trap with maximum severity will be sent to the manager. This threshold value ranges between 100 and 230 Volts.
	This command is a complete standardized implementation of the existing command set switch temperature - threshold
Syntax	`set switch power {min|max} threshold <volts (100-230)>`
Parameter	
Description	• `min` - Sets the minimum threshold power suply for the switch. When thevoltage drops below the threshold, an SNMP trap with maximum severity will be sent to the manager. • `max` - Sets the maximum threshold power suppy for the switch. When the voltage rises above the threshold, an SNMP trap with maximum severity will be sent to the manager.
Mode	Global Configuration Mode
Default	• min - 100 Volts • max - 230 Volts
Example	`Your Product(config)# set switch power min threshold 110` `Your Product(config)# set switch power max threshold 220`

Related Command(s)

- `show env` - Displays the switch related information such as CPU, Flash and RAM usage, and also displays the current power and temperature of the switch

4.41 mac-learn-rate

Command Objective This command configures the maximum number of unicast dynamic MAC (L2) MAC entries hardware can learn on the system, in a configured time interval. In next subsequent time interval, hardware can learn number of previously learnt MAC entries plus present MAC entries, this cycle will continue until MAC learning reaches to maximum number of L2 unicast dynamic entries learning capacity of the system. If rate limit is changed while timer is running, new rate limit value takes effect on next timer restart. This limit is to control the number of MAC entries indication to control plane from hardware, when hardware

MAC learning is enabled. Configuration value '0' disables this feature in the system.

The no form of the command removes the limit on number of unicast MAC entry indications (limit value is set as 0) and resets the configured time interval to default value.

This command is not supported in MBM-XEM-002.

Unsupported Commands

Syntax

```
mac-learn-rate {<no of MAC entries(0-2147483647)>} [interval {<milliseconds(1-100000)>}]

no mac-learn-rate
```

Parameter

Description

- `<no of MAC entries(0-2147483647)>` - Configures the maximum number of unicast dynamic MAC (L2) entries that can be learned in the switch within the specified time interval. The configured value takes effect on next timer restart, if this value is changed while the timer is running. This value is used to control the number of MAC entries indicated to control plane from the hardware, when hardware MAC learning is enabled. The value ranges between 0 and 2147483647. The value 0 represents that no limit is set in the switch. This limit value does not impose any

restrictions on multicast / broadcast and dynamic / static / protocol (MMRP) MAC learning capability limits.

- `interval<milliseconds(1-100000)>` - Configures the time interval (in milli-seconds) for maximum number of MAC entries to be learned in the switch. The configured value takes effect from the next timer restart. The value ranges between 1 and 100000 milli-seconds.

Mode	Global Configuration mode
Default	• <no of MAC entries(0-2147483647)> - 1000 • interval - 1000
Example	`Your Product(config)# mac-learn-rate 100 interval 500`
Related Command(s)	• `show mac-learn-rate` - Displays the maximum limit on number of MAC learning indications to control plane from hardware and the MAC learning limit rate interval.

4.42 system contact

Command Objective	This command sets the system contact information.
Syntax	`system contact <contact info>`
Mode	Global Configuration Mode
Example	`Your Product(config)# system contact support@x.com`
Related Command(s)	• `show system information` - Displays system information.

4.43 system location

Command Objective	This command sets the system location.
Syntax	`system location <location name>`
Mode	Global Configuration Mode
Example	`Your Product(config)# system location Controls`
Related Command(s)	• `show system information` - Displays system information.

4.44 clear interfaces - counters

Command Objective This command clears all the current interface counters from the interface unless the optional arguments *type* and *number* are specified to clear only a specific interface type (serial, Ethernet, Token Ring, and so on).

Syntax

```
clear interfaces [ <interface-type> <interface-id> ]
counters
```

Parameter

Description

- `<interface-type>` - Displays the IP interface configuration for the specified type of interface. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - fx-ethernet – A version of Ethernet that supports data transfer upto 25 Gigabits per second. This Ethernet supports only full duplex links.
  - cx-ethernet – A version of Ethernet that supports data transfer upto 100 Gigabits per second. This Ethernet supports only full duplex links.
  - internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.
- `<interface-id>` - Displays the IP interface configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1represents that the slot number is 0 and port number is 1.

Mode Privileged EXEC Mode

Example	`Your product# clear interfaces counters`
Related Command(s)	• `show interfaces - counters` - Displays the interface statistics for each port. • `show interfaces` - Displays the interface status and configuration

4.45 clear counters

Command Objective This command clears all the current interface counters from the interface unless the optional arguments *type* and *number* are specified to clear only a specific interface type (serial, Ethernet, Token Ring, and so on).

This command is a standardized implementation of the existing command and operates similar to that of the command clear interfaces - counters.

Syntax `clear counters [ <interface-type> <interface-id> ]`

Parameter

Description

- `<interface-type>` - Displays the IP interface configuration for the specified type of interface. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - fx-ethernet – A version of Ethernet that supports data transfer upto 25 Gigabits per second. This Ethernet supports only full duplex links.
  - cx-ethernet – A version of Ethernet that supports data transfer upto 100 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-id>` - Displays the IP interface configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1represents that the slot number is 0 and port number is 1.

Mode Privileged EXEC Mode

Example	`Your product# clear counters`

Related Command(s)	• `show interfaces counters` - Displays the interface statistics for each port. • `show interfaces` - Displays the interface status and configuration

4.46 show ip interface

Command Objective This command displays the IP interface configuration.

Syntax

```
show ip interface loopback <loopback-id(0-100)>]

show ip interface [vrf <vrf-name>] [{[Vlan <vlan-id(1-

4094)> [switch <switch-name>]] |  [<interface-type>

<interface-id>] | [loopback <loopback-id(0-100)>]}]
```

Parameter

Description

- `vrf<vrf-name>` - Displays IP interface for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
- `Vlan<vlan-id(1-4094)>` - Displays the IP interface configuration for the specified VLAN ID. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
- `switch<switch-name>` - Configures IP interface for the specified context.

  This value represents unique name of the switch context. This value is a string whose maximum size is 32 This parameter is specific to multiple.

  instance feature. This feature has been included to adhere to the Industry.

  Standard CLI syntax.
- `<interface-type>` - Displays the IP interface configuration for the specified type of interface. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.

- **<interface-id>** - Displays the IP interface configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1represents that the slot number is 0 and port number is 1.
- **loopback<loopback-id(0-100)>** - Displays the IP interface configuration for the specified loopback ID. This is a unique value that represents the specific loopback created. The value ranges between 0 and 100.

Mode Privileged EXEC Mode

Default vrf – default

☞ If executed without the optional parameters this command displays the IP interface statistics and configuration for all the available interfaces.

Example

```
Your product# sh ip interface vrf default
vlan1 is up, line protocol is up
Internet Address is 12.0.0.1/8
Broadcast Address  12.255.255.255
vlan2 is up, line protocol is up
Internet Address is 15.0.0.1/8
Broadcast Address  15.255.255.255
```

Related Command(s)

- **ip address** - Sets the IP address for an interface
- **switchport** - Configures the port as switch port
- **release** - Releases, on the specified interface, the DHCP lease obtained for an IP address from a DHCP server.
- **renew** - Renews the DHCP lease for the interface specified.
- **show interfaces** - Displays the interface status and configuration

4.47 show authorized-managers

Command Objective This command displays the configured authorized managers' related information available in the switch.

Syntax `show authorized-managers [ip-source < ip-address >]`

Parameter Description

- `ip-source< ip-address >` - Displays the configured authorized manager related information for the specified network or host address.

Mode Privileged EXEC Mode

Example

```
Your product# show authorized-managers
Ip Authorized Manager Table
---------------------------
Ip Address: 12.0.0.1
Ip Mask: 255.255.255.255
Services allowed: ALL
Ports allowed: Gi0/1

On cpu0: Deny

Vlans allowed: All Available Vlans
```

Related Command(s)

- `authorized-manager ip-source` - Configures an IP authorized manager

4.48 show interfaces

Command Objective This command displays the interface status and configuration.

Syntax

```
show interfaces [{ [<interface-type> <interface-id>]
[{ description | storm-control | flowcontrol |
capabilities | status | port-security-state }] |
{vlan <vlan-id/vfi-id> [{switch <switch-name>}]} |
tunnel <tunnel-id (0-128)> | private-vlan mapping}]
```

Parameter

Description

- `<interface-type>` - Displays the interface status and configuration for the specified type of interface. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-id>` - Displays the interface status and configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. description - Displays the admin status and protocol status for the specified interface.
- `Description -` Displays the interface description.
- `storm-control` - Displays the broadcast, multicast, and unicast storm control suppression levels for the specified interface
- `flowcontrol` - Displays the flow control related statistics information for the specified interface.

- **capabilities** - Displays the interface type, interface speed, duplex operation and flowcontrol status for the specified interface.

- **status** - Displays the status, duplex details, speed and negotiation mode of the specified interface.

- **port-security-state** - Displays the state of the port security option.

- **vlan <vlan-id/vfi-id>**- Displays the interface status and configuration for the specified VLAN/ VFI ID. This value ranges between 1 and 65535.

  – **<vlan –id>** - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094

  – **<vfi-id>**. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and

  65535. This interface type is not supported.

  The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering

  Database entries.

  VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.

  The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to the maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

- **switch<switch-name>** - Configures IP interface for the specified context.

  This value represents unique name of the switch context. This value is a string whose maximum size is 32 This parameter is specific to multiple instance feature. This feature has been included to adhere to the Industry Standard CLI syntax

- **tunnel<tunnel-id (0-128)>** - Displays the interface status and configuration for the specified tunnel ID. This is a unique

value that represents the specific tunnel created. The value ranges between 0 and 128.

- **private-vlan mapping** - Displays list of secondary Vlan to the primary vlan IVR interface, so that both VLANs share the same primary VLAN

Mode Privileged EXEC Mode

Example

```
Your product# show interfaces gigabitethernet
0/1

Gi0/1 up, line protocol is up (connected)
Bridge Port Type: Customer Bridge Port
Hardware Address is 00:01:02:03:04:22

RARP Client is enabled

MTU  1500 bytes, Full duplex, 100 Mbps,  Auto-
Negotiation

HOL Block Prevention enabled.
Invalid flowcontrol Mode

Link Up/Down Trap is enabled

Reception Counters

   Octets: 0

   Unicast Packets: 0

   Discarded Packets: 0

   Error Packets: 0

   Unknown Protocol: 0

Transmission Counters

   Octets: 8266

   Unicast Packets: 0

   Discarded Packets: 0

   Error Packets: 0

Your product# show interfaces description
```

```
Interface    Status    Protocol  Description
---------    ------    --------  -----------
Ex0/1        down      down
```

Your product# show interfaces gigabitethernet 0/2 storm control

```
Gi0/2                                                    -

DLF Storm Control: Disabled

DLF Storm Control Limit: 0

Broadcast Storm  Control:    Enabled

BroadcastStorm  Control:    0


Multicast Storm  Control:    Enabled

Multicast Storm              0
```

Your product# show interfaces gigabitethernet 0/2 flow- control

```
Port  Tx FlowControl  Rx FlowControl  Tx Pause  Rx Pause
----  --------------  -------------   --------  --------
Gi0/1    off              off             0         0
```

Your product# show interfaces gigabitethernet 0/2 capabilities

```
Gi0/2

Type: 10/100/1000 Base TX
Speed: 10, 100, 1000, Auto
Duplex: Half, Full

FlowControl: Send, Receive

Your product# show interfaces gigabitethernet 0/2
status

Port   Status       Duplex   Speed      Negotiation
----   ------       ------   ------     ------------
Gi0/2  connected    Full     100 Mbps    Auto
```

```
Your product# show interfaces vlan 1

vlan1 up, line protocol is up (connected)

Your product# show interfaces port-channel 2

po2 up, line protocol is up (connected)

Your product# show interfaces tunnel 0

tunnel0 up, line protocol is up (connected)

Hardware is Tunnel

MTU 1480 bytes

Encapsulation TUNNEL

Tunnel Source 12.0.0.2,Destination 12.0.0.3

Tunnel Protocol/transport IPV6IP Checksumming
of packets Disabled Path MTU Discovery Disabled
```

Related Command(s)

- **interface** – Enters the interface mode and allows the user to execute all the commands that supports interface configuration mode.
- **Interface-configuration and deletion** - Configures interface such as out of band management, port channel, tunnel and so on.
- **Snmp trap link-status** - Enables trap generation on the interface.
- **Storm-control** - Sets storm control rate for broadcast, multicast and DLF packets.
- **flowcontrol** - Enables flow-control.
- **show flow-control** - Displays the flow-control information.
- **mac-addr** – Configures MAC address for the interface.
- **tunnelmode** - Configures the tunnel interface with the associated parameters.
- **tunnel checksum** - Enables end-to-end checksumming of packets.
- **tunnel path-mtu-discovery** - Enables Path MTU discovery on Tunnel.

- `tunnel udlr` - Associates tunnel with a unidirectional interface.

- `shutdown – physical/VLAN/port-channel/tunnel interface` Disables a physical interface / VLAN interface / port-channel interface / tunnel interface.

4.49 show interfaces - counters

Command objectives This command displays the interface statistics for each port.

Syntax

```
show interfaces {counters | HC counters} [{
<interface- type> <interface-id> | vlan <vlan_vfi_id>
[switch <switch- name>] | tunnel <tunnel-id(0-128)> |
ppp <ppp-id(1-4094)>}]
```

Parameter

Description

- `counters` - Displays the interface statistics for all the available interfaces.
- `HC counters` -.Displays the interface incoming and outgoing traffic statistics for the for the HC port.
- `<interface-type>` - Displays the interface incoming and outgoing traffic statistics for the specified type of interface. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- `interface-id>` - Displays the counters for the interface incoming and outgoing traffic statistics for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than

  port-channel. For Example: 0/1 represents that the slot number is 0 and port number is 1. For interface type port-channel, for Example:

  1 represents port-channel ID.
- `vlan <vlan_vfi_id>` - Displays the interface statistics for the specified VLAN/ VFI ID. This value ranges between 1 and 65535.

<vlan -id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094

- **<vfi-id>**. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and

  65535, this interface type is not supported.

  The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.

  VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.

  The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based

  on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to the maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

- **switch<switch-name>** - Displays interface statistics for the specified context. This value represents unique name of the switch context. This value is a string with the maximum length as 32 This parameter is specific to multiple instance feature. This feature has been included to adhere to the Industry Standard CLI syntax

tunnel<tunnel-id(0-128)> - Displays the counters for the interface

- incoming and outgoing traffic statistics for the tunnel identifier. This is a unique value that represents the specific tunnel created. The value ranges between 0 and 128.

ppp<short(1-4094)> - Displays the counters for the interfaces of the

- point to point protocol. This value ranges between 1 and 4094.

Mode	Privileged EXEC Mode
Example	`Your Product# show interfaces counters`

```
Port       InHCOctet           InUcastPkts         InMulticastPkts
----       ---------           -----------         ---------------
Ex0/1      0                   0                   0
Ex0/2      0                   0                   0
Ex0/3      0                   0                   0
Ex0/4      0                   0                   0
Ex0/5      0                   0                   0
Ex0/6      0                   0                   0

Port       OutHCOctet          OutUcastPkts        OutMulticastPkts
----       ----------          ------------        ----------------
Ex0/1      0                   0                   0
Ex0/2      0                   0                   0
Ex0/3      0                   0                   0
Ex0/4      0                   0                   0
Ex0/5      0                   0                   0
Ex0/6      0                   0                   0
```

Related Command(s)

- `interface` - configure interface such as out of band management, port channel, tunnel and so on

4.50 show system-specific port-id

Command Objective	This command displays the system specific index configuration for all interfaces for which this configuration is done.
Syntax	`show system-specific port-id`
Mode	Privileged EXEC Mode

Example	`Your product# show system-specific port-id`
	`Interface PortID`
	`Slot0/1 45`

Related Command(s)	• `system-specific port-id` - Configures the system specific index for the port.

4.51 show custom-param

Command Objective This command displays the custom-param configurations done in the switch.

Syntax `show custom-param`

Mode Privileged EXEC Mode

Example

```
Your product# show custom-param
Slot0/1
AttrID    AttrValue
--------  --------
4         5454
Slot0/2
AttrID    AttrValue
--------  --------
2         2424
Type      Length    Value
--------  --------  --------
2         4         root
5         4         root
```

Related Command(s)

- `Set custom-param` - Configures the custom-param for a particular port.

4.52 show interface mtu

Command Objective This command shows the Maximum Transmission Unit (MTU) of ports in the switch.

Syntax

```
show interface mtu [{Vlan <vlan-id/vfi-id> [switch
<switch-name>] | port-channel <port-channel-id (1-
65535)>
| <interface-type> <interface-id> }]
```

Parameter

Description

- `Vlan <vlan-id/vfi-id>` - Displays the MTU value for the specifiedVLAN/ VFI ID. This value ranges between 1 and 65535.
  - `<vlan -id>` - VLAN ID is a unique value that represents the specific

    VLAN. This value ranges between 1 and 4094
  - `<vfi-id>`. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This createsa logical LAN for the VPLS service. This value ranges between 4096and

    65535. This interface type is not supported.

    The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering

    Database
    entries.

    VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.

    The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based

    on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs

are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

- **switch <switch-name>** - Configures IP interface for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32 This parameter is specific to multiple instance feature. This feature has been included to adhere to the Industry Standard CLI syntax
- **port-channel<port-channel-id (1-65535)>** - Displays the MTU value for the specified port-channel ID. This is a unique value that represents the specific port-channel created. This value ranges between 1 and 65535.
- **<interface-type>** - Displays the MTU value for the specified type of interface. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- **<interface-id>** - Displays the MTU value for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash.For Example: 0/1 represents thatthe slot number is 0 and port number is 1.

Mode Privileged EXEC Mode

Example

```
Your product# show interface mtu Vlan 1

vlan1    MTU size is 1500
```

Related Command(s)

- **mtu**- Configures the maximum transmission unit frame size for the interface

4.53 show interface bridge port-type

Command Objective This command displays the bridge port type of all interfaces available in the switch.

Syntax

```
show interface bridge port-type [{ port-channel
<integer

(1-65535)> | <interface-type> <ifnum> | pw <integer
(1-65535)> }]
```

Parameter

Description

- `port-channel <integer (1-65535)>`- Displays the bridge port type for the specified port-channel ID. This is a unique value that represents the specific port-channel created. This value ranges between 1 and 65535.
- `<interface-type>` - Displays the bridge port type for the specified type of interface. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<ifnum>` - Displays the bridge port type for the specified interface identifier.

  This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1.
- `pw <integer (1-65535)>` - Displays the bridge port type for the specified pseudo wire interface. This value ranges between 1 and 65535. Maximum number of PseudoWire interfaces supported in the system is100. This interface type is not supported.

Mode Privileged EXEC Mode

Example

```
Your product# show interface bridge port-
type

   Ex0/1   Bridge port type is Customer Bridge Port

   Ex0/2   Bridge port type is Customer Bridge Port

   Ex0/3   Bridge port type is Customer Bridge Port

   Ex0/4   Bridge port type is Customer Bridge Port

   Ex0/5   Bridge port type is Customer Bridge Port

   Ex0/6   Bridge port type is Customer Bridge Port
```

Related Command(s)

- `bridge port-type` - Configures the bridge port type

4.54 show nvram

Command Objective	This command displays the current information stored in the NVRAM.
Syntax	`show nvram`
Mode	Privileged EXEC Mode

Example

```
Your product# show nvram
Default IP Address: 12.0.0.5
Default Subnet Mask: 255.0.0.0
Default IP Address Config Mode: Manual
Default IP Address Allocation Protocol: DHCP
Switch Base MAC Address: 00:25:90:03:04:01
Default Interface Name: 0
Default RM Interface Name: lo:5
Config Restore Option: No restore
Config Save Option: No save
Auto Save: Disable Incremental Save: Disable
Roll Back: Enable
Config Save IP Address: 192.168.100.102
Config Save Filename: smis.conf Config Restore
Filename: smis.conf
PIM Mode: Sparse Mode
IGS Forwarding Mode: MAC based Cli
Serial Console: Yes
SNMP EngineID: 80.00.08.1c.04.46.53
SNMP Engine Boots: 55
```

```
Default VLAN Identifier: 1

Stack PortCount: 0

ColdStandby: Disable

Store Default Value: Disable

Vrf Unique Mac: Disable

Hitless Restart  Flag: Disable

Hardware Version: 1.0.2


Firmware Version: 2.0.0

Hardware Part Number: MBM-XEM-002

Software Serial Number: 1-0-0

Software Version: 6.12.0

Switch Name: SMIS

RM Heart Beat Mode: Internal

RM Redundancy Type: Hot

RM Data Plane Type: Shared

RM Type: OOB

NPAPI mode: Synchronous

TimeStamp Method: Software

Restore Flag: Disabled

Dynamic Port Count: 64

FIPS operation mode: Disabled

Restore Option: Disabled

Bridge Mode: Customer Bridge

Management Port: Disabled

Automatic Port Create Flag: Enabled
```

Related Command(s)

- `default mode` - Configures the mode by which the default interface acquires its IP address
- `default restore-file` - Configures the default restoration file
- `ip address` - Sets the IP address for an interface
- `login authentication` - Sets the authentication method for user logins
- `write` - Writes the running-config to a file in flash, startup-configuration file or to a remote site
- `erase`- Clears the contents of the startup configuration or sets parameters in NVRAM to default values
- `default ip address allocation protocol` - Configures the protocol by which the default interface acquires its IP address
- `incremental-save` - Enables/disables the incremental save feature.
- `auto-save trigger` - Enables/disables the auto save trigger function.
- `cli console` - Enables the console CLI through a serial port
- `automatic-port-create` – Enables or disables the Automatic Port Create feature.

4.55 show env

Command Objective	This command displays the status of the all the resources like CPU, Flash and RAM usage, and also displays the current, power and temperature of the switch. This command is a complete standardized implementation of the existing command.
	This command is not supported in all models.
Syntax	`show env {all | temperature | fan | RAM | CPU | flash |power}`
Parameter **Description**	• `all` - Displays threshold information of all resources such as CPU, Flash, RAM, power and temperature. • `temperature` - Displays temperature threshold values of the switch in celcius • `fan` - Displays the threshold information of the fan • `RAM` - Displays the maximum RAM usage of the switch in percentage. • `CPU` - Displays the maximum CPU usage of the switch in percentage. • `flash` - Displays the maximum flash usage of the switch in percentage. • `power` - Displays the threshold power suply for the switch
Mode	Privileged EXEC Mode

Example	`Your product# show env all`
	
	`RAM Threshold: 98%`

```
Current RAM Threshold: 97%

CPU Threshold: 92%

Current CPU Threshold: 0%

Fan Status   1: Operational
Min power supply: 110v

Max power supply: 220v

Current power supply: 230v

Max Temperature: 37C

Min Temperature: -10C

Current Temperature: 40C

Flash Threshold: 90%

Current Flash Threshold: 62%

Mgmt Port Routing: Disabled
```

Your product# show env RAM

```
RAM Threshold: 98%

Current RAM Threshold: 97%
```

Your product# show env power

```
Min power supply: 110v

Max power supply: 220v

Current power supply: 230v
```

Related Command(s)

- **set switch maximum - threshold** - Sets the switch maximum threshold values of RAM, CPU, and Flash.
- **set switch temperature - threshold** - Sets the maximum and minimum temperature threshold values of the switch.

- `set switch power - threshold` - Sets the maximum and minimum threshold values of the switch power supply.

4.56 show system information

Command Objective This command displays system information.

Syntax `show system information`

Mode Privileged EXEC Mode

Example

```
Your product# show system information
Hardware Version: 1.0.1
Firmware Version: 2.0.0
Hardware Part Number: MBM-XEM-002
Software Serial Number: 1-0-0
Software Version: 2.0.0
Switch Name: SMIS
System Contact: Supermicro
System Location: Supermicro
Logging Option: Console
Logging Login Authentication Mode: Local
Config Save Status: Not Initiated
Remote Save Status: Not Initiated
Config Restore Status: Not Initiated
Traffic Separation Control: none
```

Related Command(s)

- `login authentication` - Sets the authentication method for user logins
- `system contact` - Sets the system contact information

- `system location` - Sets the system location
- `debug-logging` - Configures the displays of debug logs.
- `config-restore` - Configures the startup configuration restore option.
- `set switch-name` - Sets the name of the switch.
- `Traffic seperation control` - Configures the method for receiving control packets to CPU.

4.57 show flow-control

Command Objective	This command displays the flow-control information.
Syntax	`show flow-control [ interface <interface-type> <interface- id>]`
Parameter	
Description	• `<interface-type>` - Displays the flow-control information for the specified type of interface. The interface can be: – qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links. – gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. – extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • `<interface-id>` - Displays the flow-control information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1represents that the slot number is 0 and port number is 1.
Mode	Privileged EXEC Mode
☞	If this command is executed without the optional parameter it displays the flowcontrol information of the switch. Otherwise it displays the flowcontrol information of the specified interface.
Example	`Your product# show flow-control interface gigabitethernet 0/2`

```
Port TxFlowControl RxFlowControl TxPause  RxPause HC TxPause HC RxPause
Gi0/2   on            on            0        0        0          0
```

Related Command(s)

- `show interfaces` - Displays interface status and configuration
- `flowcontrol` - Enables flowcontrol on an interface

4.58 show debug-logging

Command Objective This command displays the debug logs stored in file.

Syntax `show debug-logging`

Mode Privileged EXEC Mode

Example

```
Your Product(config)# debug-logging file
Your Product(config)# exit
Your product# debug spanning-tree  events
Your product# show debug-logging
console             Displays debug logs in console
flash               Displays debug logs in file
ram                 Displays debug logs in RAM disk file
(config)# debug-logging flash
(config)# exit
# debug spanning-tree events
# show debug-logging
2000-01-01 00:06:56.326688 <PLAT>   u4IfIndex = 40
u4PortCountPerslot = 2  u4Max SlotCount  = 28
i4SwitchSlotId  = 0 i4MiddleplaneId  = 129 u1BladeNodes
= 0 u 2000-01-01 00:06:57.283275 <SMGT>   <129>Jan  1
00:06:57 mus-colo-r3-smbld2-swa1  FM [FM - SYS] :
Temperature: 41 celsius crosses the threshold limit.
Min Temp 2000-01-01 00:07:02.485874 <MSR>    <129>Jan
1 00:07:02 mus-colo-r3-smbld2-swa1  FM [FM - MSR] :
Configuration restored successfully from flash. 2000-
01-01 00:07:22.486368 <SSDP>   SSDP Wait Timer End
2000-01-01 00:07:22.486445 <SSDP>
rest_bnm.c:5869:RestBnmHandleAutoJoin Not joined in BNM
NvRam: u1JoinStatus=0
```

Related Command(s)

- `debug-logging` - Configures where debug logs are to be displayed

4.59 show debugging

Command Objective	This command displays state of each debugging option.
Syntax	`show debugging`
Mode	Privileged EXEC Mode

Example	`Your product# show debugging`
	`Spanning Tree:`
	`Spanning tree timers related debugging is on`

Related Command(s)	• `debug spanning-tree` - Provides spanning tree debugging support • `debug dot1x` - Enables debugging of dot1x module • `debug radius` - Enables RADIUS debugging options • `debug ip igmp snooping`- Specifies the debug levels for the IGMP snooping module • `debug ssh` - Sets the given trace levels for SSH • `debug ssl` - Sets the given debug levels for SSL • `debug vlan` - Enables the tracing of the VLAN submodule as per the configured debug levels. • `debug garp` - Enables the tracing of the GARP submodule as per the configured debug levels. • `debug ip dhcp client` - Enables the tracking of the DHCP client operations as per the configured debug levels. • `debug ip dhcp relay` - Enables the debug level for tracing the DHCP Relay Module

- `debug ip dhcp server` - Enables the tracking of the DHCP server operations as per the configured debug levels.

4.60 show clock

Command Objective	This command displays the system date and time.
Syntax	`show clock`
Mode	Privileged EXEC Mode
Example	`Your product# show clock` `Fri Jun 28 08:31:19 2013 (UTC +05:50)`
Related Command(s)	• `clock set` - Manages the system clock

4.61 show running-config

Command Objective This command displays the configuration information currently running on the switch, the configuration for a specific interface, or map class information and this configuration is lost if the system is restarted The command is useful when there are multiple interfaces and you want to look at the configuration of a specific interface.

Syntax

```
show running-config [{ syslog | dhcp | dhcp6 | dvmrp | |
stp [ switch <context_name> ] | ecfm [switch
<context_name>] | la | pnac | igs | mlds | vlan
<vlan- id/vfi-id> [ switch <context_name> ] |
interface {
<interfacetype> <interfacenum> | vlan <vlan-id/vfi-id>}
|
ospf | isis | rip | bgp | ipv6 | rip6 | ssh | ssl | acl
|
ip | pim | pimv6 | vrrp | snmp | radius | rmon | rm |
mbsm
| ospf3 | mpls | igmp | eoam | fm | igmp-proxy | elmi |
route-map | tacacs | tac | sntp | switch
<context_name> | nat | elps | erps | [switch
<context_name>] | entity-mib | http | poe | pbb
[switch <context_name>] |cn [switch
<context_name>] | dcbx | ptp |clkiwf | mld | msdp |
msdpv6
| lldp | firewall | system | ospfte | ipsourceguard |
tlm
| rbridge | l2dhcsnp | mef | network-clock | vrf
<vrf- name> | hs | bfd | qosxtd | dsmon | mrp |
ofc}]
```

Parameter

Description

- `syslog` - Displays the configuration done in the syslog module.
- `dhcp` - Displays the configuration done in the DHCP module.
- `dvmrp` - Displays the configuration done in the DVMRP module.

- **stp** - Displays the configuration done in the STP module.

– switch <context_name> - Displays the configuration done in the context for the specified module. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

- **ecfm** - Displays the configuration done in the ECFM module.
- **la** - Displays the configuration done in the LA module.
- **pnac** - Displays the configuration done in the PNAC module.
- **igs** - Displays the configuration done in the IGS module.
- **mlds** - Displays the configuration done in the MLDS module.
- **vlan <vlan-id/vfi-id>** - Displays the configuration done for the specified VLAN / VFI ID. This is a unique value that represents the specific VLAN/ VFI created / to be created. This value ranges between 1 and 65535.

  – **<vlan -id>** - VLAN ID is a unique value that represents the specific

  VLAN. This value ranges between 1 and 4094

  – **<vfi-id>**. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and

  65535. This interface type is not supported.

  The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering

  Database
  entries.

  VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.

  The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based

  on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be

restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

- switch <context_name> - Displays the configuration done in the context for the specified module. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

- **interface -** Displays the configuration done for the specified type of interface
  - <interfacetype> - Displays the configuration done for the specified type of interface. The interface can be:
    - qx-ethernet – A version of Ethernet that supports data transfer up to 40 Gigabit per second. This Ethernet supports only full duplex links.
    - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
    - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
    - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
  - <interface-id> - Displays the configuration done for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1.
  - vlan <vlan-id/vfi-id> - Displays the configuration done for the specified VLAN / VFI ID. This is a unique value that represents the specific VLAN/ VFI created / to be created. This value ranges between 1 and 65535.
    - **<vlan –id>** - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
    - **<vfi-id>**. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

      The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.

VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.

The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to a maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

- **ospf** - Displays the configuration done in the OSPF module.
- **rip** - Displays the configuration done in the RIP module.
- **bgp** - Displays the configuration done in the BGP module.
- **ipv6** - Displays the configuration done in the IPv6 module.
- **rip6** - Displays the configuration done in the RIP6 module.
- **ssh** - Displays the configuration done in the SSH module.
- **ssl** - Displays the configuration done in the SSL module.
- **acl** - Displays the configuration done in the ACL module.
- **ip** - Displays the configuration done in the IP module.
- **pim** - Displays the configuration done in the PIM module.
- **vrrp** - Displays the configuration done in the VRRP module.
- **snmp** - Displays the configuration done in the SNMP module.
- **radius** - Displays the configuration done in the RADIUS module.
- **rmon** - Displays the configuration done in the RMON module.
- **rm** - Displays the configuration done in the RM module.
- **mbsm** - Displays the configuration done in the MBSM module.
- **ospf3** - Displays the configuration done in the OSPFv3 module.
- **mpls** - Displays the configuration done in the MPLS module.
- **igmp** - Displays the configuration done in the IGMP module.
- **eoam** - Displays the configuration done in the EOAM module.

- **fm** - Displays the configuration done in the FM module.
- **igmp-proxy** - Displays the configuration done in the IGMP proxy module.
- **elmi** - Displays the configuration done in the ELMI module.
- **route-map** - Displays the configuration done for the route map feature.
- **tacacs** - Displays the configuration done in the TACACS module.
- **tac** - Displays the configuration done in the TAC module.
- **sntp** - Displays the configuration done in the SNTP module.
- **switch <context_name>** - Displays the configuration done in the context for the specified module. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
- **nat** - Displays the configuration done in the NAT module.
- **elps** - Displays the configuration done in the ELPS module.
- **erps** - Displays the configuration done in the ERPS module.
- **switch <context_name>** - Displays the configuration done in the context for the specified module. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
- **entity-mib** - Displays the configuration done in the emtity-mib module.
- **http** - Displays the configuration done in the http module.
- **poe** - Displays the configuration done in the poe module.
- **pbb** - Displays the configuration done in the pbb module.
- **switch <context_name>** - Displays the configuration done in the context for the specified module. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
- **cn** - Displays the configuration done in the cn module.
- **switch <context_name>** - Displays the configuration done in the context for the specified module. This value represents unique name

of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

- **dcbx** - Displays the configuration done in the extended dcbx module.
- **ptp** - Displays the configuration done in the ptp module.
- **clkiwf** - Displays the configuration done in the clkiwf module.
- **mld** - Displays the configuration done in the mld module.
- **msdp** - Displays the configuration done in the msdp module.
- **msdpv6** - Displays the configuration done in the msdpv6 module.
- **lldp** - Displays the configuration done in the lldp module.
- **firewall** - Displays the configuration done in the firewall module.
- **system** - Displays the configuration done in the system.
- **ospfte** - Displays the configuration done in the OSPF TE module.
- **ipsourceguard** - Displays the configuration done in the IP Source Guard module.
- **tlm** - Displays the configuration done in the TLM module.
- **rbridge** - Displays the configuration done in the Rbridge module.
- **l2dhcsnp** - Displays the configuration done in L2 DHCP snooping module.
- **mef** - Displays the configuration done in MEF module
- **network-clock** - Displays the configuration done in SyncE module
- **vrf <vrf-name>** - Displays the configuration done for the specified VRF instance created in the system.
- **hs** - Displays the configuration done in HotSpot module
- **bfd** - Displays the configuration done in BFD module
- **qosxtd** - Displays the configuration done in QoSx module
- **qosx** - Displays the configuration done in QoS module
- **dsmon –** Displays the configuration done in DSMON module
- **mrp –** Displays the configuration done in MRP module

- `ofc` - Displays the configuration done in OFCL module

Mode Privileged EXEC Mode

☞ If executed without the optional parameters this command displays the current active configurations, other than the default configurations of all the modules in all the interfaces. Not all the features are supported at all SMIS models.

Example The output given below is only a fragment of the whole output. This output differs based on the modules that are configured.

```
Your product# show running-config stp

Building configuration...
spanning-tree mode rst
interface gigabitethernet 0/1!
interface gigabitethernet 0/2!
interface gigabitethernet 0/3!

interface gigabitethernet 0/4!
interface gigabitethernet 0/5!
interface gigabitethernet 0/6!
interface gigabitethernet 0/7!
interface gigabitethernet 0/8!
interface gigabitethernet 0/9!
interface gigabitethernet 0/10!
interface gigabitethernet 0/11!
interface gigabitethernet 0/12!

interface gigabitethernet 0/13!
interface gigabitethernet 0/14!
interface gigabitethernet 0/15!
interface gigabitethernet 0/16!
interface gigabitethernet 0/17!
interface gigabitethernet 0/18!
interface gigabitethernet 0/19!
interface gigabitethernet 0/20!
```

```
interface gigabitethernet 0/21!
interface gigabitethernet 0/22!
interface gigabitethernet 0/23!
interface gigabitethernet 0/24!
end
```

Your product# show running-config bgp

```
Building configuration...
router bgp 100

bgp router-id 100.20.6.100

bgp default ipv4-unicast

redistribute static

restart-reason softwareRestart

neighbor 100.20.6. remoteas 200
neighbor 100.20.6. update-source
neighbor 100.20.6. timers holdtime 240
neighbor 110.20.6. remote-as 300
neighbor 110.20.6. update-source
neighbor 110.20.6. timers holdtime 240!
end       20
```

Related Command(s) Related Command include the configuration commands of all the modules (given as parameters in the **`show running-config`** command)

4.62 show http server status

Command Objective	This command displays the http server status and HTTP port.
Syntax	`show http server status`
Mode	Privileged EXEC Mode

Example	`Your product# show http server status`
	`HTTP server status: Enabled`
	`HTTP port is: 80`
	`HTTP Requests In: 0`
	`HTTP Invalids: 0`

Related Command(s)	• `ip http port` – Sets the HTTP port • `set ip http` – Enables/disables HTTP

4.63 show system acknowledgement

Command Objective	This command displays acknowledgement statement for open sources used in the software.
Syntax	`show system acknowledgement`
Mode	Privileged EXEC Mode
Example	**`Your product# show system acknowledgement`**

```
  The SSH functionality in this switch is implemented
using the open source software from
http://www.openssh.org developed by Theo de Raadt,
Niels Provos, Markus Friedl,Bob Beck, Aaron Campbell
and Dug Song. All copyrights listed at
http://www.openssh.org apply.

  The SSL functionality in this switch is implemented
using the open source software from
http://www.openssl.org which include software written
by Er.c A. Young and Tim J. Hudson.All copyrights
listed at http://www.openssl.org apply.

  This switch includes cryptographic software written
by Eric A Young (eay@cryptsoft.com). This product
includes software written by Tim J. Hudson
(tjh@cryptsoft.com). PLEASE REMEMBER THAT
EXPORT/IMPORT AND/OR USE OF STRONG CRYPTOGRAPHY
SOFTWARE, PROVIDING CRYPTOGRAPHY HOOKS OR EVEN JUST
COMMUNICATING TECHNICAL DETAILS ABOUT CRYPTOGRAPHY
SOFTWARE IS ILLEGAL IN SOME PARTS OF THE WORLD. SO,
WHEN YOU IMPORT THIS PACKAGE TO YOUR COUNTRY, RE-
DISTRIBUTE IT FROM THERE OR EVEN JUST EMAIL TECHNICAL
SUGGESTIONS OR EVEN SOURCE PATCHES TO THE AUTHOR OR
OTHER PEOPLE YOU ARE STRONGLY ADVISED TO PAY CLOSE
ATTENTION TO ANY EXPORT/IMPORT AND/OR USE LAWS WHICH
APPLY TO YOU. THE AUTHORS OF OPENSSL ARE NOT LIABLE
FOR ANY VIOLATIONS YOU MAKE HERE. SO BE CAREFUL, IT IS
YOUR RESPONSIBILITY
```

Math library in this switch is implemented using the Open source software from Sun Microsystems, Inc. All copyrights listed at http://www.radiks.net/~rhuebner/mathlib.html apply.

Web Tree View Script (ftiens4.js) and Browser Detection Script (ua.js) in this switch are implemented using source code from http://www.treeview.net. All copyright listed at http://www.treeview.net apply.

4.64 show mac-learn-rate

Command Objective	This command displays maximum number of unicast dynamic MAC (L2) MAC entries hardware can learn on the system, in MAC learning limit rate interval. mac-learn-rate is not supported on some SMIS models.
Syntax	`show mac-learn-rate`
Mode	Privileged EXEC mode

Example	`Your product# show mac-learn-rate`
	`Switch MAC Learn Limit Rate :  1000`
	`Switch MAC Learn Limit Rate Interval: 1000`

Related Command(s)	• `mac-learn-rate` - Configures the number of MAC entries indication to control plane from hardware, when hardware MAC learning is enabled.

4.65 port-isolation in_vlan_ID

Command Objective	This command enables the vlan traffic to be allowed in these configured egress ports when the ingress is this interface. The no form of the command disables the Port Isolation rule in this ingress interface.

Syntax	`port-isolation in_vlan_ID [{add|remove}] port_list`
	
	`no port-isolation`

Parameter Description	• `in_vlan_ID` - Configures the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094. • `add` - Configures the addition of the egress ports • `remove` - Configures the removal of the egress ports • `port list` - Configures the list of ports through which the traffic is allowed. The ports can be either a physical or link aggregated port.
Mode	Interface configuration mode (physical ports or Link Aggregated port).
Example	`Your Product(config-if)# port-isolation 4094 add Gi0/1-10`
Related Command(s)	• `show port-isolation` - Displays the Port Isolation table

4.66 show port-isolation

Command Objective

This command displays the Port Isolation table.

Syntax

```
show port-isolation  [ingress-port <ifXtype> <ifnum>]
```

Parameter

Description

- `ingress-port` - Ingress port refers to a physical or link aggregated port through which a packet ingress.

  – `<ifXtype>` Displays the type of interface. The interface can be:

  - qx-ethernet – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.

  – `<ifnum>` Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash.

Mode

Privileged EXEC Mode

Example

```
Your product# show port isolation
```

```
Ingress Port    VlanId   StorageType   Egress List
============    ======   ===========   ===========
Gi0/2           10       Non-Volatile  Gi/1
Gi0/3           -        Non-Volatile  Gi0/2
```

Related Command(s):

- `port-isolation in_vlan_ID` - Enables the vlan traffic to be allowed in these configured egress ports when the ingress is this interface.

4.67 private-vlan mapping

Command Objective	This command maps list of secondary Vlan to the primary vlan IVR interface, so that secondary vlans can use the primary vlan IVR interface for L3 communication. The no form of the command removes all secondary VLAN association to the primary VLAN IVR interface.
	This command is not supported in all models.

Syntax	`private-vlan mapping [{add | remove}] <vlan-list>`
	
	`no private-vlan mapping`

Parameter Description

- `add` - Maps the list of configured secondary VLAN to the existing primary vlan IVR interface
- `remove` - Removes the mapping between the secondary VLAN and the primary VLAN IVR interface
- `<vlan-list>` - Configures a VLAN ID or list of VLAN IDs that should be mapped with the specified primary vlan. For Example, the value is provided as 5, 6,7 to represent the list of VLANs IDs. Specifies the vlan list for the private vlan interface.

  All existing mapped secondary vlans will be deleted.

Mode	Interface Configuration Mode
Example	`Your Product (config-if)# private-vlan mapping 18`
Related Command(s)	`show interfaces` - Displays the interface status and configuration.

4.68 audit-logging

Command Objective	This command enables or disables audit logging that allows users to configure audit trails, which track changes that have been made to a router. Each change is logged as a syslog message, and all syslog messages are kept in the audit file, which is kept in the audit subsystem.
Syntax	`audit-logging { enable | disable}`
Parameter	
Description	disable - Disables audit logging. Global Configuration Mode
Default	Disable
Example	`Your Product(config)# audit- logging enable`

Related Command(s)

- `audit-logging filename` - Specifies the name of the file to which Audit log is saved
- `audit-logging filesize` - Specifies the the maximum file size in Kilobytes of the configs.txt file
- `audit-logging reset` - Erases the contents in configs.txt file and start logging
- `show confg log` - Displays Information related to Audit Logging

4.69 audit-logging filename

Command Objective	This command specifies the name of the file to which Audit log is saved. The maximum string value of the file name is 128.
Syntax	`audit-logging filename <filename>`
Mode	Global Configuration Mode
Default	Config.txt
Example	`Your Product(config)# audit-logging filename srv.txt`
Related Command(s)	• `audit-logging` – Enables/disables audit logging • `audit-logging filesize` - Specifies the the maximum file size in Kilobytes of the configs.txt file • `audit-logging reset` - Erases the contents in configs.txt file and start logging • `show confg log` - Displays Information related to Audit Logging

4.70 audit-logging filesize

Command Objective	This command specifies the maximum file size(in Kilobytes of the configs.txt file) of the audit file which is a fixed file size in the disk file system. The audit file contains syslog messages and it is stored on the disk. The number of messages that can be stored is dependent on the size of the selected file and the size determines the number of messages that can be stored on the disk before a wraparound occurs. Ensure that the audit file is secure and the audit file should be access protected so that only the audit subsystem can access it. The value ranges between 1024 and 1048576.
Syntax	`audit-logging filesize <filesize(1024-1048576)>`
Mode	Global Configuration Mode
Default	1048576
Example	`Your Product(config)# audit-logging filesize 1025`
Related Command(s)	• `audit-logging` – Enables/disables audit logging • `audit-logging filename` - Specifies the name of the file to which Audit log is saved • `audit-logging reset` - Erases the contents in configs.txt file and start logging • `show confg log` - Displays Information related to Audit Logging

4.71 audit-logging reset

Command Objective	This command is used to erase the contents in configs.txt file and start logging.
Syntax	`audit-logging reset`
Mode	Global Configuration Mode
Example	`Your Product(config)# audit-logging reset`

Related Command(s)

- `audit-logging` – Enables/disables audit logging
- `audit-logging filesize` - Specifies the the maximum file size in Kilobytes of the configs.txt file
- `audit -logging filename` - Specifies the name of the file to which Audit log is saved
- `show confg log` - Displays Information related to Audit Logging

4.72 show config log

Command Objective	This command displays Information related to Audit Logging.
Syntax	`show config log`
Mode	Privileged EXEC Mode

Example	`Your product# show config log`
	`Audit Status: Enabled Audit`
	`File Name: config.text`
	`Audit File Size: 1025`
	`Audit Log Size Threshold: 70`

Related Command(s)

- `audit-logging` – Enables/disables audit logging
- `audit-logging filename` - Specifies the name of the file to which Audit log is saved
- `audit-logging filesize` - Specifies the the maximum file size in Kilobytes of the configs.txt file
- `audit-logging reset` - Erases the contents in configs.txt file and start logging

4.73 hol blocking prevention

Command Objective	This command enables or disables Head-of-Line Blocking prevention.
Syntax	`hol blocking prevention`
Mode	Interface Configuration Mode
Example	`Your product# hol blocking prevention`

4.74 internal-lan

Command Objective	This command adds an internal lan interface and its parameters
Syntax	`internal-lan <ilan-id (1-65535)> {add interface virtual <iface_list> | delete interface virtual <iface_list>}`
Parameter Description	• `<ilan-id (1-65535)>` - Specifies the internal lan id. The value ranges between 1 to 65535 • `add interface virtual <iface_list>` - Adds the internal lan interface and its parameters. Specifies the virtual interface • `delete interface virtual <iface_list>` - Deletes the internal lan interface and its parameters. Specifies the virtual interface
Mode	Global Configuration Mode
Example	`Your Product(config)# internal-lan 1 add interface virtual 0/1`
Related Command(s)	• `show internal-lan` – Displays the internal lan parameters.

4.75 show internal-lan

Command Objective	This command displays the internal lan parameters.
Syntax	`show internal-lan <iface_list>`
Mode	Privileged EXEC Mode
Example	`Your product# show internal-lan`
Related Command(s)	• `internal-lan`- Adds a lan interface and its parameters

4.76 show iftype protocol deny table

Command Objective	This command displays the entries of iftype protocol deny table.
Syntax	`show iftype protocol deny table [switch <context_name>]`
Parameter Description	• `switch <context_name>` - Displays iftype for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode
Example	`Your Product# show iftype protocol deny table`
Related Command(s)	• `deny iftype` – Denies the particular type of interface, bridge ports in the given protocol module, from being accessed by the protocol

4.77 clear line vty

Command Objective	This command clears the console or virtual terminal line to an idle state. If AAA authorization is enabled, it will allow the user have the administrator privilege (15) to use this command. Otherwise, it only allows the administrator user to use this command.
Syntax	`clear line vty {<line-number(2-9)> | all}`
Parameter Description	• `<line-number(2-9)>` - Clears the vty information of the specified telnet session. This value ranges between 2 and 9. • `all` - Clears all the vty information.
Mode	Privileged EXEC Mode
Example	`Your Product# clear line vty 2`
Related Command(s)	• `show line` ---Displays the TTY line information • `aaa authorization` – Enable AAA authorization

4.78 tunnel hop-limit

Command Objective	This command configures Hop Limit on Tunnel. The hop limit value ranges between 0 and 255. The value of the Hop Limit field specifies the maximum number of routers that an IPv6 packet can pass through before the packet is considered invalid.
Syntax	`tunnel hop-limit <0-255>`
Mode	Interface configuration mode (Tunnel)
☞	This command executes only if the tunnel interface is configured

Example	`Your Product(config)# interface tunnel 1`
	
	`Your Product(config-if)# tunnel mode ipv6ip config-id 1 source vlan1 dest 10.203.113.114`
	
	`Your Product(config-if)# tunnel hop-limit 5`

Related Command(s)	• `tunnel mode` - Configures the tunnel interface with the associated parameters

4.79 login block-for

Command Objective	This command configures the maximum number of successful login attempts and the lock out time to block the user.
Syntax	`login block-for <seconds(30-600)> attempts <tries(1-10)>`
Parameter Description	• `<seconds(30-600)>` - Configures the lock out time in seconds that a user is blocked following unsuccessful logins. This value ranges between 30 and 600. • `<tries(1-10)>` - Configures login attempts. This is the number of times a user is allowed to login using wrong password in the login prompt. This value ranges between 1 and 10.
Mode	Global Configuration mode
Default	• seconds - 30 • tries - 3
Example	`Your Product(config)# login block-for 30 attempts 3`

4.80 audit-logging logsize-threshold

Command Objective	This command configures the threshold value of the log storage space with respect to the maximum storage space size. The threshold value in percentage ranges between 1 and 99.
Syntax	`audit-logging logsize-threshold <threshold in %(1-99)>`
Mode	Global Configuration mode
Default	threshold in % - 70
Example	`Your Product(config)# audit-logging logsize-threshold 99`
Related Command(s)	`show config log` - Displays the information related to Audit Logging.

4.81 feature telnet

Command Objective	This command enables the telnet service in the system. The no form of this command disables the telnet service.
Syntax	`feature telnet` `no feature telnet`
Mode	Global Configuration mode
Default	The telnet service is enabled
Example	`Your Product(config)# feature telnet`

Related Command(s)

- `show telnet server` - Displays the telnet server status.

4.82 show telnet server

Command Objective	This command displays the telnet server status.
Syntax	`show telnet server`
Mode	Privileged EXEC Mode
Example	`Your Product# show telnet server` `telnet service enabled`
Related Command(s)	• `feature telnet` - Enables the telnet service in the system.

4.83 show audit

Command Objective	This command displays the content of the audit-log file.
Syntax	`show audit`
Mode	Privileged EXEC Mode

Example	**`Your Product# show audit`**
	`Audit:ADMIN audit logging reset21:27:54 2011SUCCESS CONSOLE Fri Jun 10`
	`Audit:ADMIN firewall  SUCCESS CONSOLE Fri Jun 10 21:27:57 2011`
	`Audit:ADMIN enable SUCCESS CONSOLE Fri Jun 10 21:27:58 2011`
	`Audit:ADMIN end SUCCESS CONSOLE Fri Jun 10 21:28:01 2011`
	`Audit:ADMIN c t SUCCESS CONSOLE Fri Jun 10 21:28:04 2011`
	`Audit:ADMIN enable password level 5 Password123$ SUCCESS CONSOLE Fri Jun 10 21:28:45 2011`
	`Audit:ADMIN end SUCCESS CONSOLE Fri Jun 10 21:28:46 2011`

4.84 set http authentication-scheme

Command Objective	This command configures the Configurable HTTP authentication scheme.
Syntax	`set http authentication-scheme {default | basic | digest}`
Parameter Description	• `default` - Sets the configurable HTTP authentication scheme to default. • `basic` - Sets the configurable HTTP authentication scheme to basic. • `digest` - Sets the configurable HTTP authentication scheme to digest.
Mode	Global Configuration Mode
Default	`default`
Example	`Your Product (config)# set http authentication-scheme basic`
Related Command(s)	• `show http authentication-scheme` - Displays the Operational andConfigurable authentication scheme values.

4.85 set http redirection enable

Command Objective	This command enables the HTTP redirection feature. The no form of this command disables the HTTP redirection feature.

Syntax	`set http redirection`
	
	`enable no http`
	
	`redirection enable`

Mode	Global Configuration Mode
Default	HTTP redirection is disabled
Example	`Your Product (config)#  set http redirection enable`

4.86 http redirect

Command Objective This command configures the alternate server for the URL specified. The alternate server's IP or Domain name can be specified. On receiving request for the URL, a redirection status is sent as response for the request.

The no form of this command removes the redirection entry added to the server specified for the URL.

Syntax

```
http redirect <URL to be redirected> server {IPv4
Address|IPv6 Address | Domain name}

no http redirect [<URL to be redirected>]
```

Parameter

Description

- `<URL to be redirected>` - Configures the URL which has to be redirected.
- `server` - Configures the server for the URL which is redirected. The options are:
  - `IPv4 Address` – Sets the IP address of the alternate server in v4 format
  - `IPv6 Address` – Sets the IP address of the alternate server in v6 format
  - `Domain name` - Configures the domain name of the alternate server

Mode Global Configuration Mode

Example Your Product (config)# http redirect /sample/ server 12.0.0.2

Related Command(s)

- `show http redirection` - Displays the redirection entries filtered by URL or all the entries.

4.87 show http authentication-scheme

Command Objective	This command displays the operational and configurable authentication scheme values.
Syntax	`show http authentication-scheme`
Mode	Privileged EXEC Mode

Example	`Your Product# show http authentication-scheme`
	`The Operational HTTP authentication scheme is Digest`
	`The Configured HTTP authentication scheme is Digest`

Related Command(s)	`set http authentication-scheme` – Sets the Configurable HTTP Authentication scheme value to default or basic or digest.

4.88 show http redirection

Command Objective This command displays the redirection entries filtered by URL or all the entries.

Syntax `show http redirection [URL]`

Parameter Description

- `URL` - Configures the URL for which the redirection entry has to be displayed.

Mode Privileged EXEC Mode

Example

```
Your Product# show http redirection /sample/

HTTP Redirection Entries

-----------------------------

URL                              Server IP/DomainName

---                              --------------------

/sample/                         12.0.0.2
```

Related Command(s)

- `http redirect` - Configures the alternate server for the URL specified.

4.89 ENTITY MIB

Entity MIB is a standardized way of representing a single agent, which supports multiple instances of one MIB. With the Entity MIB support in SMIS, all the instances of the MIBs registered with agent are identifiable, so that the NMS (Network Management System) can easily communicate with the particular instance / logical entity. Entity MIB also provides the complete hierarchal hardware component view to the user.

The list of CLI commands for the configuration of ENTITY MIB is as follows:

- `set entity physical-index`
- `show entity logical`
- `show entity physical`
- `show entity lp-mapping`
- `show entity alias-mapping`
- `show entity phy-containment`

4.90 set entity physical-index

Command Objective This command configures the read-write objects of the physical components present in the system which defines a greater than zero value used to identify a physical entity. The physical index is an arbitrary value that uniquely identifies the physical entity which can be small positive integer.

Syntax

```
set entity physical-index <integer (1..2147483647)>

{[asset-id <SnmpAdminString (Size (1..32))>] [serial-
number

<SnmpAdminString (Size (1..32))>] [alias-name

<SnmpAdminString (Size (1..32))>] [uris <OCTET-STRING
(Size(1..255))>]}

no entity physical-index <integer (1-2147483647)>
[assetId] [serial-number][alias-name][uris]
```

Parameter

Description

- `<integer(1..2147483647)>` - Specifies the Index of the physical entity.The value ranges between 1 and 2147483647
- `asset-id` - Specifies the asset tracking identifier for the physical entity. This value is a string of size varying between 1 and 32 characters. Asset tracking identifier is not needed for the physical entities (such as repeater ports within a repeater module) that are not considered as a field replaceable unit by the vendor. A zero-length string is returned for these entities.
- `serial-number` - Specifies the vendor-specific serial number string for the physical entity. This value is a string of size varying between 1 and 32 characters. Serial number string is not needed for the physical entities (such as repeater ports within a repeater module) that are not considered as a field replaceable unit by the vendor. A zero-length string is returned for these entities.
- `alias-name` - Specifies the alias name for the physical entity. This value provides a non-volatile handle for the entity. This value is a string of size varying between 1 and 32 characters.

- **uris** - Specifies the additional identification information (that is URI (Uniform Resource Indicator) about the physical entity. This value ranges between 1 and 255.

Mode Global Configuration mode

Default

- **assetId** - Zero-length string, on initial instantiation of the physical entity.
- **serial-number** - Zero-length string, on initial instantiation of the physical entity, if a serial number is unknown or non-existent. Correct vendor- assigned serial number, on initial instantiation of the physical entity, if the serial number is available to the SNMP agent.
- **alias-name** - Zero-length string, on initial instantiation of the physical entity. The SNMP agent may also set the value to a locally unique default value.

- If write access is implemented for an instance of asset ID and a value is written into the instance, SNMP agent should retain the value as long as the entity associated with the instance remains instantiated. This instantiation includes the instantiation across all re-initialization / reboot of the NMS. and instantiation resulting in a change of the physical entity's index value.
- If write access is implemented for an instance of the serial number string and a value is written into the instance, SNMP agent should retain the value as long as the entity associated with the instance remains instantiated. This instantiation includes the instantiation across all re-initialization / reboot of the NMS. and instantiation resulting in a change of the physical entity's index value.
- If the agents cannot provide non-volatile storage for the serial number string, then the agents are not required to implement write access for the the serial number string object.
- Implementations that can correctly identify the serial numbers of all installed physical entities are not required to provide write access to the serial number string object
- If write access is implemented for an instance of the alias name and a value is written into the instance, SNMP agent should retain the value as long as the entity associated with the instance remains instantiated. This instantiation includes the instantiation across all re-

initialization / reboot of the NMS. and instantiation resulting in a change of the physical entity's index value.

Example

```
Your Product(config)# set entity physical-index
2222222 asset-id 8 serial-number 7 alias-name GJG
uris yg
```

Related Command(s)

- `show entity physical` - Displays the physical entities

4.91 show entity logical

Command Objective

This command displays multiple logical entities within a single physical entity.

The overall physical entity contains multiple (smaller) physical entities and each logical entity is associated with a particular physical entity.

Syntax

```
show entity logical [index <integer (1..2147483647)>]
```

Parameter Description

- `index<integer (1..2147483647)>` - Displays the index of the logical entity. The value ranges between 1 and 2147483647.

Mode

Privileged EXEC Mode

Example

```
Your product#  show entity logical index 1

Logical Index: 1

Logical Description: SMIS
Logical Type: stdpnac
Logical Community: default
Logical Transport Address:
Logical Transport Domain:

Logical Context Engine Id: 80:00:08:1c:04:46:64
Logical Context Name: default
```

Related Command(s)

- `set entity physical-index` - Configures the read-write objects of the physical components present in the system.

4.92 show entity physical

Command Objective This command displays the physical entities which are physical components that represents an identifiable physical resource within a managed system. Zero or more logical entities may utilize a physical resource at any given time.

Syntax

```
show entity physical [index <integer (1..2147483647)>]
```

Parameter Description

- **index<integer (1..2147483647)>** - Displays the index of the physical entity. The value ranges between 1 and 2147483647.

Mode Privileged EXEC Mode

Example

```
Your product# show entity physical index 1
Physical Index: 1
Physical Descr: Network Element
Physical VendorType: Supermicro
Physical ContainedIn: 0
Physical Class: 3
Physical ParentRelPos: 0
Physical Name: SMIS
Physical HardwareRev: 1.0.2
Physical SoftwareRev: 2.0.0
Physical FirmwareRev: 2.0.0
Physical Serial Num: MBM-XEM-002
Physical MfgName: Supermciro
```

```
Physical ModelName:
Physical Alias: DummyName
Physical AssetID: assetId
Physical MfgDate: 2009-8-6,13:30:30.0,-4:0
Physical Uris:
Physical FRU Status: 1
```

Related Command(s)

- `interface-configuration and deletion` - Configures interface such as out of band management, port channel, tunnel and so on
- `set entity physical-index` - Configures the read-write objects of the physical components present in the system

---

4.93 show entity lp-mapping

Command Objective This command displays the mapping of logical and physical entities, interfaces, and non-interface ports managed by a single agent. The LPMapping contains mappings between logical entities and physical components supporting that entity. A logical entity can map to more than one physical component, and more than one logical entity can map to the same physical component.

Syntax

```
show entity lp-mapping
```

Mode Privileged EXEC Mode

Example

```
Your product#  show entity lp-mapping
Logical Index - 1 is mapped to Physical Index- 10
Logical Index - 1 is mapped to Physical Index- 11
Logical Index - 2 is mapped to Physical Index- 10
Logical Index - 2 is mapped to Physical Index- 11
Logical Index 3 is mapped to Physical Index10
```

Related Command(s)

- `map switch` - Maps the port to the Context

4.94 show entity alias-mapping

Command Objective This command displays the mapping of logical and physical entity with alias external object identifiers values. This allows resources managed with other MIBs (e.g. repeater ports, bridge ports, physical and logical interfaces) to be identified in the physical entity hierarchy.

Each alias identifier is only relevant in a particular naming scope.

Syntax

```
show entity alias-mapping [index <integer
(1..2147483647)>]
```

Parameter

Description

- `index <integer (1..2147483647)>` - Displays the Index of the physical entity. The value ranges between 1 and 2147483647.

Mode Privileged EXEC Mode

Example

```
Your product# show entity alias-mapping

Physical Index 10 for all Logical entities is mapped
to external identifier : Gi0/1

Physical Index - 11 for all Logical entities is
mapped to external identifier : Gi0/24
```

Related Command(s)

- `interface – configuration and deletion` - Configures interface such as out of band management, port channel, tunnel and so on.

4.95 show entity phy-containment

Command Objective This command displays the simple mapping between the physical contained values for each container/containee relationship in the managed system.

Syntax `show entity phy-containment [index <integer (1..2147483647)>]`

Parameter Description

- `index <integer (1..2147483647)>` - Displays the Index of the physical entity. The value ranges between 1 and 2147483647.

Mode Privileged EXEC Mode

Example

```
Your product#  show entity phy-containment
Containmaint Relationship
-------------------------

Physical Entity            : 1 (Stack)
Member Physical Entities   : 2 (Power Supply), 3 (Cpu), 4 (Fan)
                             5 (Fan), 6 (Fan), 7 (Fan)
                             8 (Fan), 9 (Chassis)

Physical Entity            : 9 (Chassis)
Member Physical Entities   : 10 (Module)

Physical Entity            : 10 (Module)
```

```
Member Physical Entities   : 11 (Port), 12 (Port), 13 (Port)
                             14 (Port), 15 (Port), 16 (Port)
                             17 (Port), 18 (Port), 19 (Port)
                             20 (Port), 21 (Port), 22 (Port)
                             23 (Port), 24 (Port), 25 (Port)
                             26 (Port), 27 (Port), 28 (Port)
                             29 (Port), 30 (Port), 31 (Port)
                             32 (Port), 33 (Port), 34 (Port)
                             35 (Port), 36 (Port), 37 (Port)
                             38 (Port), 39 (Port), 40 (Port)
                             41 (Port), 42 (Port), 43 (Port)
                             44 (Port), 45 (Port), 46 (Port)
                             47 (Port), 48 (Port), 49 (Port)
                             50 (Port), 51 (Port), 52 (Port)
                             53 (Port), 54 (Port), 55 (Port)
                             56 (Port), 57 (Port), 58 (Port)
                             59 (Port), 60 (Port), 61 (Port)
                             62 (Port), 63 (Port), 64 (Port)
                             65 (Port), 66 (Port), 67 (Port)
                             68 (Port), 69 (Port), 70 (Port)
                             71 (Port), 72 (Port), 73 (Port)
                             74 (Port), 75 (Port), 76 (Port)
                             77 (Port), 78 (Port), 79 (Port)
                             80 (Port)
-------------------------------------------------------------
```

Related Command(s)

- `interface – configuration and deletion` - Configures interface such as out of band management, port channel, tunnel and so on

4.96 set hitless-restart enable

Command Objective	This command enables the hitless restart feature by which the software is restarted without affecting any datapath and without disturbing the protocol relationships with any peer nodes. This command is not supported.
Syntax	`set hitless-restart enable`
Mode	Privileged EXEC Mode
Default	Hitless restart is disabled.

Example	**`Your Product#  set hitless-restart enable`**
	`<129>Nov  9 04:54:50 SMIS FM [FM - RM] : 131.0.0.1`
	`RM :ACTIVE completed started none :: Nov  9 04:54:49 2011`
	`SMIS# Nov 9 04:54:49 2011: RM[ACTIVE]:`
	`Hitless Restart: Bulk storage completed.Nov  9 04:54:49 2011: RM[ACTIVE]:`
	`Hitless Restart: Steady state pkt request starts. Nov  9 04:54:49 2011: RM[ACTIVE]:`
	`Hitless Restart: All Steady State packets are stored in NPSIM.Nov  9 04:54:49 2011: RM[ACTIVE]:`
	`Do write start-up and PLEASE RESTART THE EXE`

4.97 speed

Command Objective This command sets the speed of the interface and FEC mode.

The “no” form of the command restores the default settings.

Syntax

```
speed { 10 | 100 | 1000 | 10000 | 25000 | 40000 | 50000
| 56000 | 100000 } [ { auto | fec { cl91 | cl74 | cl108
| off } } ]
```

Parameter

Description

- `10` - Sets the port to run at 10Mbps.
- `100` - Sets the port to run at 100Mbps.
- `1000` - Sets the port to run at 1000Mbps.
- `10000` - Sets the port to run at 10Gbps.
- `25000` - Sets the port to run at 25Gbps.
- `40000` - Sets the port to run at 40Gbps.
- `50000` - Sets the port to run at 50Gbps.
- `56000` - Sets the port to run at 56Gbps.
- `100000` - Sets the port to run at 100Gbps
- `auto` - Detects and sets fec mode automatically based on the peer switch.
- `fec` – set the forward error correction mode of the port.
- `Cl91` – enable rs-fec on 100Gbps port.
- `Cl74` – enable base-r fec on 25 or 50Gbps port.
- `Cl108` – enable re-fec on 25Gbps port.
- `off` – disable fec.

Mode Interface Configuration Mode

Example

```
Your Product(config-if)# speed 25000 fec off
```

4.98 automatic-port-create

Command Objective	This command enables or disables the Automatic Port Create feature. This configuration takes effect only after system restart.
	To create or delete ports at STP module level, the Automatic Port Create feature has to be disabled.
Syntax	`automatic-port-create { enable | disable }`
Parameter **Description**	• `enable` - Enables Automatic Port Create feature and the ports are automatically created in STP module when it is mapped to a context. • `disable` - Disables Automatic Port Create feature. When set to disabled, ports are not created automatically and ports can be created at STP.
Mode	Global Configuration Mode
Default	enable
Example	`Your Product(config)# automatic-port-create enable`
Related Command(s)	• `spanning-tree - Properties of an interface` - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled. • `show nvram` – Displays the current information stored in the NVRAM.

- `write start-up config` – Writes the running-config to a flash file, startup-configuration file or to a remote site

4.99 port-type providerInstancePort

Command Objective	This command configures the PIP (Provider Instance Port) type. PIP is nothing but a Backbone Edge Bridge Port that can receive and transmit I-tagged frames for multiple customers. PIPs are applicable only on PBB I Components.
Syntax	`port-type providerInstancePort`
Mode	Interface Configuration Mode (Physical/ Portchannel)
☞	This command executes only if • PBB functionality is started in the bridge. • Bridge Mode is Provider backbone bridge I-Component mode
Example	`Your Product(config-if)# port-type providerInstancePort`
Related Command(s)	• `no shutdown provider-backbone-bridge` – Initializes the PBB feature in the bridge. • `set gmrp disable` – Globally disables GMRP feature on all ports of a switch. • `set gvrp disable` – Globally disables GVRP feature on all ports of a switch. • `shutdown garp` – Shuts down the GARP module in the switch on all ports and releases all memories used for the GARP module. • `shutdown spanning-tree` – Shuts down spanning tree functionality in the switch. • `no ethernet cfm start` – Shuts down an Ethernet CFM processing on the switch. • `bridge-mode` - Sets the bridge mode of the Switch Provider as Backbone Bridge I component Mode.

4.100 sleep

Command Objective	This command makes the SMIS to sleep for the given time. Sleep delays the SMIS CLI thread for the configured seconds. This value ranges between 1 and 65535in seconds.
Syntax	`sleep <seconds(1-65535)>`
Mode	Privileged EXEC Mode
Example	`Your Product# sleep 51`

4.101 rate-limit pause

Command Objective	This command enables the pause ingress rate limit above which PAUSE frames are transmitted on the interface. The no form of the command disables pause ingress rate limiting on a port.

Syntax	`rate-limit pause [<high-watermark>] [<low-watermark>]`
	
	`no rate-limit pause`

Parameter **Description**	• <high-watermark> - Configures the ingress rate equal to or above which PAUSE frames are transmitted. This value ranges between 1 and 80000000 kbps • <low-watermark> - Configures the ingress rate below which transmission of PAUSE frames are stopped. This value ranges between 1 and 80000000 kbps. This parameter is not supported in all SMIS models.
Mode	Interface Configuration Mode (Physical)
Example 300000	`Your Product (config-if)# rate-limit pause 400000`

4.102 cpu controlled learning

Command Objective	This command enables software learning of MAC Address from the packets arriving on the interface instead of hardware learning of MAC address. The no form of the command disables CPU controlled learning of MAC Address on the interface.

Syntax	`cpu controlled learning`
	
	`no cpu controlled learning`

Mode	Interface Configuration Mode (Physical)
Example	`Your Product (config-if)# cpu controlled learning`

4.103 traffic-separation control

Command Objective This command configures the method for receiving control packets to CPU.

This control ensures that the CPU processing capacity is utilized appropriately, according to the need of the protocol.

Syntax

```
traffic-separation control {system_default |
user_defined | none}
```

Parameter

Description

- `System_default` - Configures the method for receiving control packets to CPU as system default. This implies that the software can automatically install the ACL and QoS rules for all the control packets.

If the configuration is changed from 'system_default' to 'user_defined' option, then all the default ACL/QoS rules for carrying protocol control packets to CPU are removed. Then user has to install the specific ACL/QoS rules, to carry the intended control packets to CPU for the processing.

- `User_defined` - Configures the method for receiving control packets to CPU as user defined. This implies that the software cannot automatically install the ACL and QoS rules for all the control packets. Only the administrator can install the required rules for receiving control packets to CPU

If the configuration is changed from 'user-defined' to system-default or none, all the default ACL filters are installed. Already existing (if any) user configured ACL rules in the system are not removed.

- `none` - Configures the method for receiving control packets to CPU as none.

If the configuration is changed from 'none' to 'system_default' option, then all the default ACL filters for carrying protocol control packets to CPU are removed and new set of filters will be installed. Each filter will be associated with Qos rules.

If the configuration is changed from 'none' to 'user_defined' option, then all the default ACL filters for carrying protocol control packets to CPU are removed. Then user has to install the specific ACL/QoS rules, to carry the intended control packets to CPU for the processing.

Mode	Global Configuration Mode
Default	none
Example	`Your Product (config)# traffic-separation control system_default`

Related Command(s)

- `show access-lists` - Shows the configuration details.

4.104 mdix auto

Command Objective	This command enables the MDI/MDIX Auto Crossover of the interface The no form of the command disables the MDI/MDIX Auto Crossover of the interface and set the port as MDIX port.

Syntax	`mdix auto`
	
	`no mdix auto`

Mode	Interface Configuration Mode
Default	AutoCross is disabled
Example	`Your Product(config-if)# mdix auto`
Related Command(s)	• `set port` - Sets the port to MDI or MDIX mode

4.105 set port

Command Objective	This command sets the port to MDI or MDIX mode. This command is hardware specific and mdix is the vice versa of mdi.
Syntax	`set port { mdi | mdix }`
Parameter Description	• `mdi` – Sets the port to mdi mode. This is hardware specific where transmit pair are pins 1,2 and the receive pair are 3,6 pins respectively for the particular port. • `mdix` - Sets the port to mdix mode. This is hardware specific where transmit pair are pins 3, 6 and the receive pair are 1, 2 pins respectively for the particular port. mdix is the vice versa of mdi
Mode	Interface Configuration Mode
☞	This command executes only when Auto cross is disabled.
Example	`Your Product(config-if)# set port mdix`
Related Command(s)	• `mdix port` - Enables the MDI/MDIX Auto Cross over of the interface

4.106 config-restore

Command Objective	This command configures the startup configuration restore option. This feature is not available in some SMIS models.
Syntax	`config-restore {flash | remote ip-addr <ip-address> file <filename> | norestore | ztp}`
Parameter Description	• `flash` - Restores the flash file that is to be used for restoration when the system is restarted • `remote ip-addr <ip-address>` - Restores the IP address of the remote system from where the switch configurations have to be downloaded to the 'Startup Configuration File' in the flash. • `file <filename>` - Restores the specified remote location file that is to be used for restoration. This is a string with maximum size as 12. • `norestore` - Specifies that the switch configurations need not be restored when the system is restarted. • `ztp` – Restore the configurarion from a DHCP server with Zero Touch Provisioning function
Mode	Privileged EXEC Mode
Default	norestore
Example	`Your Product# config-restore flash`
Related Command(s)	• `show system information` – Displays the system information.

4.107 set switch-name

Command Objective	This command sets the name of the switch. This is a string with a maximum size of 15. The “no” form of the command restores the default switch name.

Syntax	`set switch-name <switchname>`
	
	`no switch-name`

Mode	Global Configuration mode
Example	`Your Product(config)# set switch-name sw1`
Related Command(s)	• `show system information` – Displays the system information

4.108 packet receive index

Command Objective This command configures the packet pattern and mask for pattern matching on the received packets.

Syntax

```
packet receive index <integer (0-4)> {value | mask|port <port_list>} no packet receive index <integer(0-4)> [ mask ]
```

Parameter Description

- <integer (0-4)> -Configures the packet receive index value whichuniquely identifies a pattern to be matched. This value ranges between 0 and 4.
- `value` - Sets a value for the pattern to match with the received packets.
- `mask` - Sets a value to mask the received packets. This value is the mask for the pattern to be matched by the packet analyser. This value ranges between 1 and 1600.
- `port <port_list>` - Configures the port / list of ports of the receiver pattern. This is the complete set of ports over which the pattern is to be matched by the packet This value ranges between 1 and 320. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.

Mode Global Configuration Mode

Example

```
Your Product(config)# packet receive index 0 port 223
```

Related Command(s)

- `show packet receive` - Displays the match ports and the timers of the Pattern Analyser.

4.109 packet send index port

Command Objective	This command sets the port, interval, count for the packet transmitter and transmits the packet provided the packet pattern is configured. The no form of the command disables the packet transmitter for given index

Syntax	`packet send index <integer (0-4)> port <port_list> [count <integer (0-65536)> [interval <integer (1-65535)>]]`
	
	`no packet send index <integer(0-4)>`

Parameter **Description**	• `<integer (0-4)>` -Configures the packet send index value whichuniquely identifies a packet to be sent. This value ranges between 0 and 4. • `port <port_list>` - Configures the port or port list of the receiver pattern. This value ranges between 1 and 320. Use comma as a separator without space while configuring list of interfaces. Example: 1,3. • `count <integer (0-65536)>` - Configures the number of packet to be sent over the ports. This value ranges between 0 and 65536. • `interval <integer (1-65535)>` - Configures the time interval for sending the packet over the port in seconds. This value ranges between 1 and 65535.
Mode	Global Configuration Mode
Example	`Your Product(config)# packet send index 1 port 5`
Related Command(s)	`show packet send index` - Displays the values of the packet transmitter table.

4.110 packet send index value

Command Objective	This command sets the packet pattern for the packet transmitter and transmits the packet, provided the interface is configured. The packet send index ranges between 0 and 4 and the packet send value ranges between 1 and 1600. The no form of the command disables the packet transmitter for given index.

Syntax	`packet send index <integer (0-4)> value`
	
	`no packet send index <integer (0-4)>`

Mode	Global Configuration Mode

Example	`Your Product(config)# packet send index 1 value`
	
	`Enter Value: 4`

Related Command(s)	`show packet send index` - Displays the values of the packet transmitter table.

4.111 show packet send index

Command Objective	This command displays the values of the packet transmitter table. The packet send index ranges between 0 and 4.
Syntax	`show packet send index <integer(0-4)>`
Mode	Privileged EXEC Mode

Example	`Your Product# show packet send index 1`
	`Index: 1`
	`Value of the Pkt:`

Related Command(s)	• `packet send index value` - Sets the port, interval, count for the packet transmitter and transmits the packet provided the packet pattern is configured. • `packet send index port` - Sets the packet pattern for the packet transmitter and transmits the packet, provided the interface is configured.

4.112 show packet receive index

Command Objective	This command displays the values of the packet receiver table. The packet receive index ranges between 0 and 4.
Syntax	`show packet receive index <integer(0-4)>`
Mode	Privileged EXEC Mode

Example	`Your Product# show packet receive index 1`
	
	`Packet Analyzer`

Related Command(s)	`packet receive index` - Configures the packet pattern and mask for pattern matching on the received packets.

4.113 set mirroring

Command Objective	This command enables or disables the mirroring in the system
Syntax	`set mirroring {enable | disable}`
Parameter Description	• `enable` – Enables mirroring in the system. When set as enabled all mirroring configurations present will be programmed in hardware. • `disable` – Disables mirroring in the system and removes all configuration from the hardware
Mode	Global Configuration Mode
Default	enable
Example	`Your Product(config)# set mirroring enable`
Related Command(s)	• `show monitor all` - Displays the mirroring information present in the system.

4.114 default exec-timeout

Command Objective	This command configures the default exec-timeout value for line disconnection. This value ranges between 1 and 18000 seconds.
Syntax	`default exec-timeout <integer (1-18000)>` `no default exec-timeout`
Mode	Global Configuration Mode
Example	`Your Product(config)# default exec-timeout 5`

4.115 ip unnumbered

Command Objective

This command configures the associated source interface for the unnumbered interface. This enables to communicate over unnumbered interface with the peer using source address as any one of the associated IP address configured to other interfaces.

The no form of the command removes associated source interface for the unnumbered interface.

Syntax

```
ip unnumbered ([<peer-mac>] [{[vlan <vlan-id/vfi-id>] | [<iftype> <ifnum>] | [loopback <loopback-id(0-100)>]}])

no ip unnumbered ([<peer-mac>] [{[vlan <vlan-id/vfi-id>] | [<iftype> <ifnum>] | [loopback <loopback-id(0-100)>]}])
```

Parameter

Description

- `<peer-mac>` - Configures the unicast peer mac address for unnumbered interface. This needs to be configured for proper forwarding of IP packets over unnumbered interfaces.
    - `vlan <vlan-id/vfi-id>` - Configures the unnumbered interface for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
        - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
        - `<vfi-id>`. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

            The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.

            VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.

The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

- **<iftype>** - Configures the associated source address for the specified type of interface. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- **<ifnum>** - Configures the associated source interface for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1.
- **loopback <loopback-id(0-100)> -** Configures the associated source address for the specified loopback. This value ranges between 0 and 100

Mode	Interface Configuration Mode (VLAN)

☞	The interface should be shutdown before executing this command.

Example

Unnumbered interface for VLAN

```
Your Product(config)# int vlan 1

Your Product(config-if)# ip address 14.0.0.1 255.0.0.0

Your Product(config)# int vlan 2
```

```
Your Product(config-if)# ip unnumbered vlan 1
```

Unnumbered interface for unicast peer mac address

```
Your Product(config)# int vlan 1

Your Product(config-if)# ip address 14.0.0.1 255.0.0.0

Your Product(config)# int vlan 2

Your Product(config-if)# ip unnumbered
00:01:02:03:04:02
```

Related Command(s)

- `ip address` - Configures IP address for an interface.

4.116 clear http server statistics

Command Objective	This command clears the HTTP server requests received and discarded statistics.
Syntax	`clear http server statistics`
Mode	Global Configuration Mode
Example	`Your Product(config)# clear http server statistics`

4.117 show license

Command Objective	This command shows the license status for particular switch models. When the switch is not licensed, and be locked in User EXEC Mode, this command will show the license application data on the screen, and users can copy the output of this command to send to technical support for licensing.
Syntax	`show license`
Mode	User EXEC Mode

Example	**`Your Product> show license`**
	`Hardware Version: P6-01`
	`Switch Serial Number: SSG36BR06B99988`
	`Switch MAC Address: 00-25-90-FF-FF-FF`
	`Hardware Part Number: SSE-G3648BR`
	`License: Absent`
	`Fingerprint:`
	`{2bpfav0cGQyxDQavEQ4ADxYZGQsSDAEKGAQQGhYZGQwBChAaCAoQCAgIGAcWCAgSBxQSEwgSEAcSAxgSChQWBRsEAQUCFAUSGBMKARIJCQsKEhADAhgSCAQICAcICBsTBQoKmfPGxPjBpPLw8fbFx4WDlsKJYPn1lGqX9OLZww==}`

4.118 install license

Command Objective	This command installs license file or license code to activate the switch. Only applicable to particular models.
Syntax	`install license {tftp://ip-address/filename | usb:filename | code <license-code>}`
Mode	User EXEC Mode

Example

```
Your Product> install license code

16586b36b83ecb81bf03e4ea5eb8619dea80302acf2d22f958a131a
a9adc63f30e267c9a7e14a25ae79f12c916cc31bb459be7431e9121
35e7dce40c3f9539dd0946757c981b531379445c2b7248d81abff4b
696f16f86e32257a4ceeff83f7e3d2c4a218732976c360aba35af2c
8bbee05f2cd67e43d438e35bc77adae0b42bee63583a8e483c6f400
5f9ddc0c1fad814ba73cf162818cbdad9f822f6bbfb588620115a52
978125c3819e8419a96867ca019c429bf12a5c4bf3e31b977e445d4
e9a4e8f3ea61e05b2852f6a1df6b2c780c6fb0d15724536c035c245
1e9c8350f1f6b535fff3941e5981732355330483ffa0b63a21e6300
24d3b4d1ed064a98e

License code validated, activation procedure completed.

Operation successfully completed.

Rebooting the system...

Your Product> install license usb:my_license.lic

License code validated, activation procedure completed.

Operation successfully completed.

Rebooting the system...

Your Product> install license
tftp://192.168.100.200/my_license.lic

License code validated, activation procedure completed.

Operation successfully completed.
```

```
Rebooting the system...
```

4.119 uninstall license

Command Objective	This command deactivates the switch by removing the license. Only applicable to particular models.
Syntax	`uninstall license`
Mode	Global Configuration Mode

Example	`Your Product(config)# uninstall license`
	`This command will delete the license and reboot`
	`the system, do you really want to proceed? [y/n]`
	`License data cleared, rebooting the system...`

4.120 copy debug-files

Command Objective	Copy debug info files to a remote site or usb storage.
Syntax	`copy debug-files {tftp://ip-address/filename | sftp://<user-name>:<pass-word>@ip-address/filename | usb:filename}`
Parameter Description	• `tftp://ip-address/filename` - Configures the TFTP details for taking back up of system logs in TFTP server. – ip-address - the IP address or host name of the TFTP server. – filename - The name of the file in which the system logs should be stored. Filenames and directory names are case sensitive • `sftp://<user-name>:<pass-word>@ip-address/filename` - Configures the SFTP details for taking back up of system logs in SFTP server. – `user-name` - The user name of remote host or server. – `pass-word` – The password for the corresponding user name of remote host or server. – `ip-address` - The IP address or host name of the server. – `filename` - The name of the file in which the system logs should be stored. Filenames and directory names are case sensitive
Mode	All Modes
Example	`Your Product# copy debug-files tftp://10.0.0.10/test`

4.121 multiplex

Command Objective	Set internal ports or external SFP+ ports switching.
Syntax	`multiplex {internal | external}`
Parameter	
Description	• This command is to configures internal or external port switching. Those Interanl ports 17 to 20 and external ports 25 to 28 share the same ASIC ports. Multiplex is set in external mode; Those internal ports 17 to 20 will be disabled. Multiplex is set in internal mode; Those external ports 25 to 28 will be disabled. To take effect, switch should be restarted after configuration. – `internal` - The multiplex flag is to set in internal ports. – `external` – The multiplex flag is to set in external ports.
Mode	Global Configuration Mod
Example	`Your Product#multiplex  external`

4.122 ip mtu

Command Objective	This command configures the IP MTU over router port. The value ranges from 1280 to 9216.
Syntax	`ip mtu <frame-size(1280-9216)>`
Mode	Interface Configuration Mode This command is applicable only for router port.
Default	1500
☞	• The value includes the length etherfame header. • The value should be small than or equal to L2 MTU. • Need to configure both “mtu” and “ip mtu” to route jumbo frame over router port.
Example	`Your Product(config-if)# ip mtu 900`

Related Command(s)

- `show interfaces` - Displays the interface status and configuration
- `show interface mtu` - Displays the global maximum transmission unit

4.123 aaa authentication login ascii-authentication

Command Objective	This command allows ASCII authentication for passwords on remote login authentication. This feature only supports to TACACS server. The no form of this command reverts to its default value (PAP)

Syntax	`aaa authentication login ascii-authentication`
	
	`no aaa authentication login ascii-authentication`

Mode	Global Configuration Mode
Default	no aaa authentication login asci-authentication
Example	`Your Product(config)# aaa authentication login asci-authentication`

Related Command(s)

- `login authentication` – Sets the authentication method for user logins

4.124 aaa authentication login default group

Command Objective	This command configures the authentication method list for user logins. This command dose the same thing with “loging authenticate” except this one supports specifying a server group. These two commands overwrite each other, and dose not show in the running config at the same time. If all AAA authorization servers down or doesn’t reply, it allows the user fallback to local authentication. The no form of this command revert to its default value (local)

Syntax	`aaa authentication login default [group {tacacs | radius | <group-name(31)>}] [local]`
	
	`no aaa authentication login default`

Parameter
 	
Description
	• `group –` Use the group methods.
	  • `tacacs –` Use all Tacacs+ hosts for the group.
	  • `radius –` Use all Radius hosts for the group.
	  • `<group-name(31)> –` Use the server group with the name. A server group can be created with the command “aaa group server”. If the server group dose not exists when doing authentication, the user can not login, or fallback to local authenticate if configured.
	• `local –` Use local authentication. If both group methods and local are configured, then local authenticate is performed after all group methods do not respond.

Mode	Global Configuration Mode
Default	aaa authentication login default local

Example	`Your Product(config)# aaa authentication login default group tacacs local`

Related Command(s)

- `login authentication` – Sets the authentication method for user logins
- `aaa group server` – Create a server group

4.125 aaa group server tacacs+

Command Objective

This command creates a TACACS+ server group and enter TACACS+ server group configuration mode.

The no form of this command deletes the server group.

Syntax

```
aaa group server tacacs+ <group-name(31)>

no aaa group server tacacs+ <group-name(31)>
```

Parameter Description

- `<group-name(31)>` – The TACACS+ server group name.

Mode

Global Configuration Mode

Example

```
Your Product(config)# aaa group server tacacs+ TacServer1

Your Product(config-tacacs+)#
```

Related Command(s)

- `server` – Add a server to TACACS+ server group
- `show tacacs` – Displays the statistical log information and server for TACACS+ client

4.126 server

Command Objective	This command adds a server to the TACACS+ server group. The no form of this command deletes the server from the server group.

Syntax	`server {<ipv4-address> | <ipv6-address>}`
	
	`no server {<ipv4-address> | <ipv6-address>}`

Parameter **Description**	• `<ipv4-address>` - IP address of the server. The server must be already configured with “tacacs-server host”. • `<ipv6-address>` - IPv6 address of the server. The server must be already configured with “tacacs-server host”.
Mode	TACACS+ server group configuration mode

Example	`Your Product(config)# tacacs-server host 10.1.2.3 key 123456`
	
	`Your Product(config)# aaa group server tacacs+ TacServer1`
	
	`Your Product(config-tacacs+)# server 10.1.2.3`

Related Command(s)	• `aaa group server` – Create a server group • `show tacacs` - Displays the statistical log information and server for TACACS+ client • `tacacs-server host` - configures the TACACS server with the parameters

4.127 ztp

Command Objective	This command enables or disables the Zero Touch Provisioning feature after reloading the switch. ZTP can do a firmware upgrade and download the switch configuration from the DHCP server when the switch starts up.
Syntax	`ztp {enable | disable}`
Parameter	
Description	• `enable` – enable Zero Touch Provisioning function when switch starts up. • `disable` – disable ZTP.
Mode	Global Configuration Mode
Example	`Your Product(config)# ztp enable` `Your Product(config)# ztp disable`
Related Command(s)	• `show nvram` – Displays the current information stored in the NVRAM • `config-restore` – Configures the startup configuration restoration option

5 RADIUS

RADIUS (Remote Authentication Dial-In User Service), widely used in network environments, is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for embedded network devices such as routers, modem servers, switches and so on. RADIUS is currently the de-facto standard for remote authentication. It is very prevalent in both new and legacy systems. It is used for several reasons:

- RADIUS facilitates centralized user administration (Authentication, Authorization and Accounting).
- RADIUS consistently provides some level of protection against an active attacker.

The list of CLI commands for the configuration of RADIUS is as follows:

- radius-server host
- debug radius
- show radius server
- show radius statistics

☞ The privilege level though RADIUS is not supported.

5.1 radius-server host

Command Objective

This command configures the RADIUS client with the parameters (host, timeout, key, retransmit).

The no form of the command deletes RADIUS server configuration.

Syntax

```
radius-server host {ipv4-address | ipv6-address |
host- name} [auth-port <integer(1-65535)>] [acct-
port <integer(1-65535)>] [timeout <1-120>]
[retransmit <1-254>] [key<secret-key-string>]
[primary]

no radius-server host {ipv4-address | ipv6-address
| host- name} [primary]
```

Parameter

Description

- `ipv4-address` - Configures the IPv4 address of the RADIUS server host.
- `ipv6-address` - Configures the IPv6 address of the RADIUS server host.
- `host-name` - Configures the DNS (**Domain Name System)** name of the RADIUS server host. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
- `auth-port <integer(1-65535)>` - Configures a specific UDP (**User Datagram Protocol)** destination port on this RADIUS server to be used solely for the authentication requests. The value of the auth port ranges between 1 and 65535.
- `acct-port <integer(1-65535)>` - Configures a specific UDP destination port on this RADIUS to be solely used for accounting requests. The value of the auth port ranges between 1 and 65535.
- `timeout <1-120>` – Configures the time period in seconds for which a client waits for a response from the server before re-ransmitting the request. The value of the time out in ranges between 1 to 120 in seconds.
- `retransmit <1-254>` - Configures the maximum number of attempts the client undertakes to contact the server. The value number of retransmit attempts ranges between 1 and 254.

- **key <secret-key-string>** - Configures the Per-server encryption key which specifies the authentication and encryption key for all RADIUS communications between the authenticator and the RADIUS server. The value of the maximum length of the secret key string is 46.
- **primary** - Sets the RADIUS server as the primary server. Only one server can be configured as the primary server, any existing primary server will be replaced, when the command is executed with this option.

Mode Global Configuration Mode

Default

- timeout - 10 seconds
- retransmit - 3 attempts
- key - empty string

Example

```
Your Product (config)# radius-server host 10.0.0.1 key
pass
```

Related Command(s)

- **aaa authentication dot1x default** - Enables the dot1x local authentication or RADIUS server based remote authentication method for all ports
- **show radius server** - Displays RADIUS server configuration
- **show radius statistics** - Displays RADIUS statistics

5.2 debug radius

Command Objective	This command enables RADIUS debugging options. The radius debug traces capture error information and failure messages in the server. These are registered in a log file for future reference. Each trace has to be enabled individually. The no form of the command disables RADIUS debugging options.
Syntax	`debug radius {all | errors | events | packets | responses | timers} no debug radius`
Parameter **Description**	• `all` - Generates traces for all the RADIUS server messages • `errors` - Generates traces for error code messages. All the instances where an error is identified are captured by this trace. The error is registered in the log. • `events` - Generates traces for events related messages. Events like authentication query from authenticator, response from server are registered in the log. • `packets` - Generates traces for number of packets, kind of packets received and sent from server. • `responses` - Generates traces for responses sent from the server to authenticator. • `timers` - Generates traces for the different timers used in the session before the system is reboot.
Mode	Privileged EXEC Mode
Default	Debugging is Disabled
Example	`Your Product# debug radius all`

5.3 show radius server

Command Objective	This command displays RADIUS server Host information which contains, Index, Server address, Shared secret, Radius Server status, Response Time, Maximum Retransmission, Authentication Port and Accounting Port.
Syntax	`show radius server [{<ucast_addr> | <ip6_addr> | <string>}]`
Parameter	
Description	• `<ucast_addr>` - Displays the related information of the specified unicast address of the RADIUS server host. • `<ip6_addr>` - Displays the related information of the specified IPv6 address of the RADIUS server host. • `<string>` - Displays the name of the RADIUS server host. This maximum value of the string is of size 32.
Mode	Privileged EXEC Mode

Example	**`Your Product# show radius server`**
	`Primary Server: 2005::33`
	`Radius Server Host Information Index: 1`
	`Server address: 13.0.0.100`
	`Shared secret: SupermicroRADIUS`
	`Radius Server Status: Enabled`
	`Response Time: 10`
	`Maximum Retransmission: 3`
	`Authentication Port: 1812`
	`Accounting Port: 1813`

```
Index: 2

Server address: 2005::33

Shared secret: SupermicroRADIUS
Radius Server Status: Enabled

Response Time: 10

Maximum Retransmission: 3

Authentication Port: 1812

Accounting Port: 1813

-----------------------------------------
```

Related Command(s)

- `radius-server host` - Configures the RADIUS client with the parameters

5.4 show radius statistics

Command Objective	This command displays RADIUS Server Statistics for the data transfer between server and the client from the time of initiation.
Syntax	`show radius statistics`
Mode	Privileged EXEC Mode

Example	**`Your Product# show radius statistics`**
	`Radius Server Statistics`
	`-------------------------`
	`Index: 1`
	`Radius Server Address: 10.0.0.1`
	`UDP port number: 1812`
	`Round trip time: 0`
	`No of request packets: 8`
	`No of retransmitted packets: 80`
	`No of access-accept packets: 0`
	`No of access-reject packets: 0`
	`No of access-challenge packets: 0`
	`No of malformed access responses: 0`
	`No of bad authenticators: 0`
	`No of pending requests: 97`
	`No of time outs: 89`
	`No of unknown types: 0`
	`-------------------------------------------`

Related Command(s)

- `radius-server host` - Configures the RADIUS client with the parameters

6 TACACS

TACACS (Terminal Access Controller Access Control System), widely used in network environments, is a client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for providing NAS (Network Access Security). NAS ensures secure access from remotely connected users. TACACS implements the TACACS Client and provides the AAA (Authentication, Authorization and Accounting) functionalities.

TACACS is used for several reasons:

- Facilitates centralized user administration.
- Uses TCP for transport to ensure reliable delivery.
- Supports inbound authentication, outbound authentication and change password request for the Authentication service.
- Provides some level of protection against an active attacker.

The list of CLI commands for the configuration of TACACS is as follows:

- `tacacs-server host`
- `tacacs use-server address`
- `tacacs-server retransmit`
- `aaa authorization`
- `aaa accounting`
- `debug tacacs`
- `show tacacs`
- `show accounting`

6.1 tacacs-server host

Command Objective	This command configures the TACACS server with the parameters (host, timeout, key) and specifies the IP address of one or more TACACS and it specifies the names of the IP host or hosts maintaining a TACACS+ server. The no form of the command deletes server entry from the TACACS server table.

Syntax	`tacacs-server host {<ipv4-address> | <ipv6-address> | <host-name>} [single-connection] [port <tcp port (1-65535)>] [timeout <time out in seconds(1-255)>] {key <secretkey>}`
	
	`no tacacs-server host { <ipv4-address> | <ipv6-address>}`

Parameter Description	• `<ipv4-address>` - Configures the IPv4 address of the host. • `<ipv6-address>` - Configures the IPv6 address of the host • `<host-name>` - Configures the DNS (Domain Name System) name of the TACACS server host. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported. • `single-connection` - Allows multiple sessions to be established over a single TCP connection for AAA functionalities • `port<tcp port (1-65535 )>` - Configures the TCP port number in which the multiple sessions are established. The value ranges between 1 and 65535. • `timeout<time out in seconds(1-255)>` -Configures the time period (in seconds) till which a client waits for a response from the server before closing the TCP connection. The link between the server and the client gets disconnected, if the specified time is exceeded. The value ranges from 1 to 255 seconds. • `key<secret key>` - Specifies the authentication and encryption key for all TACACS communications between the authenticator and the TACACS server. The value is string of maximum length 64.
Mode	Global Configuration mode
Default	• port – 49 • timeout - 5 seconds

Example	`Your Product (config)# tacacs-server host 12.0.0.100`
	
	`TACACS+ server configured with default secret key !`

	Your Product (config)# tacacs-server host 2005::33 TACACS+ server configured with default secret key !
Related Command(s)	• **show tacacs** - Displays the server (such as IP address, Single connection, Port and so on) and statistical log information (such as Authen. Starts sent, Authen. Continues sent, Authen. Enables sent, Authen. Aborts sent and so on) for TACACS+ client. • **tacacs use-server address** - Selects the server for the user from the list of configured servers.

6.2 tacacs use-server address

Command Objective	This command configures the server IP address and an active server from the list of servers available in the TACACS server table. The no form of the command disables the configured client active server.

Syntax	`tacacs use-server address { <ipv4-address> | <ipv6- address>}`
	
	`no tacacs use-server`

Parameter Description	• `<ipv4-address>` - Configures the IPv4 address of the host. • `<ipv6-address>` - Configures the IPv6 address of the host.
Mode	Global Configuration mode
☞	The specified ip address should be any one of the entries from the TACACS server table
Example	`Your Product (config)# tacacs use-server address 10.0.0.100`
Related Command(s)	• `show tacacs` - Displays the server (such as IP address, Single connection, Port and so on) and statistical log information (such as Authen. Starts sent, Authen. Continues sent, Authen. Enables sent, Authen. Aborts sent and so on) for TACACS+ client. • `tacacs-server host` - Creates the TACACS server entry in a TACACS server table. • `tacacs-server retransmit` - Configures the retransmit value which is the time interval(in seconds) till which the client waits for a response from active server.

6.3 tacacs-server retransmit

Command Objective	This command configures the retransmit value. It is the number of times the client searches the active server from the list of servers maintained in the TACACS client, when active server is not configured. The retransmit value ranges from 1 to 100 The no form of the command resets the retransmit value to its default value
Syntax	`tacacs-server retransmit <retries>` `no tacacs-server retransmit`
Mode	Global configuration mode
Default	2
Example	`Your Product (config)# tacacs-server retransmit 3`
Related Command(s)	• `tacacs use-server address` - Selects an active server from the list of servers available in the TACACS server table.

6.4 aaa authorization

Command Objective	This command enables the aaa authorization feature for TACACS. It only supports those sessions connected from console, Telnet and SSH. The no form of the command disables the aaa authorization feature for TACACS. If AAA authorization is enabled, the user only could get the privilege from AAA authorization server. If AAA authorization server downs or doesn't reply, it allows the user fallback the privilege from local account when user enable AAA authorization fallback local otherwise it will set the privilege as 1. If AAA authorization server reply authorization failed, it will set the privilege as 1. When enable AAA authorization, it will allow the users have the administrator privilege (15) to use administrator commads, for example: username and clear line. When disable AAA authorization, it only allows the administrator user to use those commads

Syntax	`aaa authorization group {tacacs | <group-name(31)>} [local]`
	
	`no aaa authorization group {tacacs | <group-name(31)>}`

Parameter Description	• `tacacs` - Use all configured TACACS servers. • `<group-name(31)>` - Use the server group with the name. • `local` - Allow user fallback the privilege from local account.
Mode	Global configuration mode
Default	AAA authorization is Disabled
Example	`Your Product (config)# aaa authorization group tacacs local`
Related Command(s)	• `show tacacs` - Displays the server (such as IP address, Single connection, Port and so on) and statistical log information (such as Authen. Starts sent, Authen. Continues sent, Authen. Enables sent, Authen. Aborts sent and so on) for TACACS+ client. • `aaa group server tacacs+` - Creates a server group • **enable** - Enters to privileged EXEC mode. • `clear line vty` - Clears the console or virtual terminal line to an idle state.

6.5 aaa accounting

Command Objective	This command enables the aaa accounting feature for TACACS. It only supports those sessions connected from console, Telnet and SSH. The no form of the command disables the aaa accounting feature for TACACS. AAA accounting allows user to track the usage of accessing switches. When AAA accounting is activated, the network access server (NAS) reports user activity to the TACACS+ security server in the form of accounting record, depending on which method user have implemented. The accounting records contain accounting (attribute, value) pairs and are stored in the security server.

Syntax	`aaa accounting [exec] [commands {<level (0-15)> | all}] default [{start-stop | stop-only}] group {tacacs | <group-name(31)>}`
	
	`no aaa accounting default group {tacacs | <group-name(31)>}`

Parameter Description	• **exec** - Runs accounting for EXEC shell session. • **commands {<level (0-15)> | all}** - the switch sends the accounting information for all the executed commands at the specified privilege level, the valid privilege level entries are from 0 through 15, or all for all levels. • **start-stop** - Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. • **stop-only** - Sends a stop accounting notice at the end of the requested user process. • **tacacs** - Use all configured TACACS servers. • **<group-name(31)>** - Use the server group with the name.
Mode	Global configuration mode
Default	• AAA accounting is Disabled • Send accounting information for all command levels • Send stop-only accounting notice at the end of the requested user process
Example	`Your Product (config)# aaa accounting exec commands all default stop-only group tacacs`
Related Command(s)	• **show accounting** - Display aaa accounting settings. • **show tacacs** - Displays the server (such as IP address, Single connection, Port and so on) and statistical log information (such as Authen. Starts sent, Authen. Continues sent, Authen. Enables sent, Authen. Aborts sent and so on) for TACACS+ client. • **aaa group server tacacs+** - Creates a server group • **enable** - Enters to privileged EXEC mode.

6.6 debug tacacs

Command Objecti	This command sets the debug trace level for TACACS client module. The no form of the command disables the debug trace level for TACACS client module.

Syntax	`debug tacacs { all | info | errors | dumptx | dumprx | accounting }`
	
	`no debug tacacs`

Parameter Description	• **all** - Generates debug messages for all possible traces (Dumptx, Dumprx, Error, Info) • **info** - Generates debug statements for server information messages such as TACACS session timed out, server unreachability, Session ID exceeded and so on. • **errors** - Generates debug statements for error debug messages such as failure caused during packet transmission and reception. • **dumptx** - Generates debug statements for handling traces. This trace is generated when there is an error condition in transmission of packets. • **dumprx** - Generates debug statements for handling traces. This trace is generated when there is an error condition in reception of packets. • **accounting** - Generates debug statements for accounting traces. This trace is generated when there is an accounting activity.
Mode	Privileged EXEC Mode
Default	Debugging is Disabled
Example	`Your Product# debug tacacs all`

6.7 show tacacs

Command Objective	This command displays the server (such as IP address, Single connection, Port and so on), the Authorization status and statistical log information (such as Authen. Starts sent, Authen. Continues sent, Authen. Enables sent, Authen. Aborts sent and so on) for TACACS+ client. This command can also displays the TACACS server groups.
Syntax	`show tacacs [server-groups [<group-name(31)>]]`
Parameter Description	• `server-groups` – Display all server groups, or the specified server group with the name. • `<group-name(31)>` - Display the server group with the name.
Mode	Privileged EXEC Mode
☞	It displays the information only for the servers configured in the TACACS server table.

```
Your Product# show tacacs
TACACS client routing-context : mgmt
Server : 1
Server address        : 1.1.1.3
Address Type          : IPV4
    User Enabled Single Connection   : yes
    Server Support Single Connection : unknown
    TCP port        : 49
    Timeout         : 5
    Secret Key      :
Server : 2
Server address        : 1.1.1.4
Address Type          : IPV4
    User Enabled Single Connection   : yes
    Server Support Single Connection : unknown
    TCP port        : 49
    Timeout         : 5
    Secret Key      :
Authorization         : Disable
Authen. Starts sent   : 8
Authen. Continues sent : 0
Authen. Enables sent  : 0
Authen. Aborts sent   : 0
Authen. Pass rvcd.    : 0
Authen. Fails rcvd.   : 3
Authen. Get User rcvd. : 0
Authen. Get Pass rcvd. : 0
Authen. Get Data rcvd. : 0
```

	Authen. Errors rcvd. : 0 Authen. Follows rcvd. : 0 Authen. Restart rcvd. : 0 Authen. Sess. timeouts : 0 Author. Requests sent : 0 Author. Pass Add rcvd. : 0 Author. Pass Repl rcvd : 0 Author. Fails rcvd. : 0 Author. Errors rcvd. : 0 Author Follows rcvd. : 0 Author. Sess. timeouts : 0 Acct. start reqs. sent : 0 Acct. WD reqs. sent : 0 Acct. Stop reqs. sent : 0 Acct. Success rcvd. : 0 Acct. Errors rcvd. : 0 Acct. Follows rcvd. : 0 Acct. Sess. timeouts : 0 Malformed Pkts. rcvd. : 5 Socket failures : 0 Connection failures : 0
Related Command(s)	• **tacacs-server host** – Creates a TACACS server entry in a TACACS Server • **tacacs use-server address** – Configures an active server from the list of servers available in the TACACS server table • **aaa authorization** – Enable AAA authorization • **aaa group server tacacs+** - Creates a server group

6.8 show accounting

Command Objective	This command displays the accounting settings.
Syntax	`show accounting`
Mode	Privileged EXEC Mode

Example	`Your Product# show accounting`
	`Accounting Enable`
	`Command Privilege : All`
	`Send Type : STOP-only`

7 SSH

SSH (Secure Shell) is a protocol for secure remote login and other secure network services over an insecure network. It consists of three major components:

- The Transport Layer Protocol provides server authentication, confidentiality and integrity.
- The User Authentication Protocol authenticates the client-side user to the server. It runs over the transport layer protocol.
- The Connection Protocol multiplexes the encrypted tunnel into several logical channels. It runs over the user authentication protocol.

The client sends a service request once a secure transport layer connection has been established. A second service request is sent after user authentication is complete. This allows new protocols to be defined and coexist with these protocols.

The list of CLI commands for the configuration of SSH is as follows:

- `ip ssh`
- `ssh`
- `debug ssh`
- `show ip ssh`
- `ip ssh transport-max-allowed bytes`
- `ip ssh pubkey-chain`
- `ssh server-address`
- `show ssh-configurations`

7.1 ip ssh

Command Objective

This command configures the various parameters associated with SSH server.

The standard port used by SSH is 22. SSH server allows remote and secure configuration of the switch. The SSH server provides protocol version exchange, data integrity, cipher and key exchange algorithms negotiation between two communicating entities, key exchange mechanism, encryption and server authentication. The auth takes values as bit mask. Setting a bit indicates that the corresponding MAC-list will be used for authentication.

The no form of this command re-sets the various parameters associated with SSH server.

Syntax

```
ip ssh {version compatibility | cipher ([des-cbc] [3des- cbc] [aes128-cbc] [aes256-cbc]) | auth ([hmac-md5] [hmac- sha1]) }

no ip ssh {version compatibility | cipher ([des-cbc] [3des- cbc] [aes128-cbc] [aes256-cbc]) | auth ([hmac-md5] [hmac- sha1]) }
```

Parameter

Description

- `version compatibility` - Configures the version of the SSH. When set to true, it supports both SSH version-1 and version-2. When set to false, it supports only the SSH version-2
- `cipher` - Configures the Cipher-List. This cipherlist takes values as bit mask. Setting a bit indicates that the corresponding cipher-list is used for encryption.

  – `des-cbc` – This is a 1 bit cipherlist. It is based on a symmetric-key algorithm that uses a 56-bit key.

  – `3des-cbc` – This is a 0 bit cipherlist. Triple DES provides a relatively simple method of increasing the key size of DES to protect against brute force attacks, without requiring a completely new block cipher algorithm.

– **aes128-cbc** – This is a 2-bit cipherlist. Advanced Encryption Standard (AES) is a specification for the encryption of electronic data for 128 bits

– **aes256-cbc** - This is a 3-bit cipherlist Advanced Encryption Standard (AES) is a specification for the encryption of electronic data for 256 bits

- **auth** - Configures Public key authentication for incoming SSH sessions.

Mode Global configuration Mode

Default

- version compatibility – False
- cipher - 3des-cbc
- auth - hmac-sha1

Example

```
Your Product (config)#ip ssh  version compatibility

Your Product (config)# ip ssh cipher des-cbc
```

Related Command(s)

- **show ip ssh** - Displays SSH server information.
- **ip ssh**- Enables or disables the ssh subsystem.
- **ssh** - Enables or disables the ssh subsystem

7.2 ssh

Command Objective	This command either enables or disables the ssh subsystem. When set to enable, the switch is accessible through ssh from a remote location. Setting ssh to disable, removes the ssh access to the switch.
Syntax	`ssh {enable | disable}`
Parameter **Description**	• `enable` - Enables the ssh subsystem. • `disable` - Disables the ssh subsystem.
Mode	Global configuration Mode
Default	enable
Example	`Your Product# ssh enable`
Related Command(s)	• `ip ssh` - Configures the various parameters associated with SSH server

7.3 debug ssh

Command Objective	This command enables the trace levels for SSH. System errors such as memory allocation failures are notified using LOG messages and TRACE messages. Interface errors and protocol errors are notified using TRACE messages. Setting all the bits will enable all the trace levels and resetting them will disable all the trace levels The no form of this command re-sets the SSH trace levels.

Syntax	`debug ssh ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer] [server])`
	
	`no debug ssh ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer] [server])`

Parameter **Description**	• `all` - Generates debug statements for all traces. • `shut` - Generates debug statements for shutdown traces. This trace is generated on successful shutting down of SSH related module and memory. • `mgmt` - Generates debug statements for management plane functionality traces. • `data` - Generates debug statements for data path • `ctrl` - Generates debug statements for Control Plane functionality traces • `dump` - Generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets. • `resource` - Generates debug statements for traces with respect to allocation and freeing of all resource except the buffers. • `buffer` - Generates debug statements for traces with respect to allocation and freeing of buffer. • `server` - Generates debug statements while creating/ opening/ closing SSH server sockets and any failures to wake up SSH server sockets. Also generates debug statements during enabling /disabling of SSH server.

Mode	Privileged EXEC Mode
Default	Debugging is Disabled
Example	`Your Product# debug ssh all`
Related Command(s)	• `show ip ssh` - Displays SSH server information

7.4 show ip ssh

Command Objective	This command displays the SSH server information such as version, cipher algorithm, authentication and trace level.
Syntax	`show ip ssh`
Mode	Privileged EXEC Mode

Example	`Your Product# show ip ssh`
	`Version: 2`
	`Cipher Algorithm: 3DES-CBC`
	`Authentication: HMAC-SHA1`
	`Trace Level: None`
	`Max Byte Allowed:32768`

Related Command(s)	• `ip ssh` - Enables SSH server on the device and configures the various parameters associated with SSH server • `debug ssh` - Enables the trace levels for SSH. • `ip ssh transport-max-allowed bytes` - configure the maximum number of bytes allowed in an SSH transport connection

7.5 ip ssh transport-max-allowed bytes

Command Objective	This command configures the maximum number of bytes allowed in an SSH transport connection. The maximum allowed bytes ranges between 1 and 32768. The SSH connection will be allowed only if the packet size does not exceed the value configured and is dropped if the value exceeds the configured.
Syntax	`ip ssh transport-max-allowed bytes <integer(1-32768)>`
Mode	Global configuration Mode
Example	`Your Product# ip ssh transport-max-allowed bytes 1`
Related Command(s)	• `show ip ssh` - Displays SSH server information

7.6 ip ssh pubkey-chain

Command Objective	This command configures the SSH clients public key, to be used for public key-based authentication. The no form of the command disables the SSH clients public key that is to be used for public key-based authentication.

Syntax	`ip ssh pubkey-chain`
	
	`no ip ssh pubkey-chain`

Mode	Privileged EXEC Mode
Example	`Your Product# ip ssh pubkey-chain`
Related Command(s)	• `show ip ssh` - Displays SSH server information

7.7 ssh server-address

Command Objective	This command configures the SSH server listening IP address and the primary port number.
Syntax	`ssh server-address <ip-address> [port <integer(1-65535)>]`
Parameter Description	• `server-address <ip-address>` - Configures the listening IP address on the SSH server. • `port <integer(1-65535)>]` - Configures the primary port number on which SSH server listens. This value reanges between 1 and 65535.
Mode	Global Configuration Mode
Default	Port - 22
Example	`Your Product (config)# ssh server-address 12.0.0.0 port 1`
Related Command(s)	• `show ssh-configurations` - Displays the SSH server listening IP and port informations.

7.8 show ssh-configurations

Command Objective	This command displays the SSH server listening IP address and port information.
Syntax	`show ssh-configurations`
Mode	Privileged EXEC Mode

Example	`Your Product# show ssh-configurations`
	`SSH Listening IP 12.0.0.0`
	`Port 1`

Related Command(s)	• `ssh server-address` - Configures the SSH server listening IP address and the primary port number

8 SSL

SSL (Secure Sockets Layer), is a protocol developed for transmitting private documents through Internet. It works by using a private key to encrypt data that is transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:

The SSL Protocol is designed to provide privacy between two communicating applications (a client and a server) and is designed to authenticate the server, and optionally the client. SSL requires a reliable transport protocol (for Example, TCP) for data transmission and reception.

The advantage of the SSL Protocol is that it is application protocol independent. A higher level application protocol (for Example, HTTP, FTP, TELNET and so on.) can layer on top of the SSL Protocol transparently. The SSL Protocol can negotiate an encryption algorithm and session key as well as authenticate a server before the application protocol transmits or receives its first byte of data. All of the application protocol data is transmitted encrypted, ensuring privacy.

The list of CLI commands for the configuration of SSL is as follows:

- `ip http secure`
- `ssl gen cert-req algo rsa sn`
- `ssl server-cert`
- `debug ssl`
- `show ssl server-cert`
- `show ip http secure server status`
- `version`
- `show restconf status`
- `restconf enable`

8.1 ip http secure

Command Objective

This command enables SSL server on the device and also configures ciphersuites and crypto keys.

The no form of the command disables SSL server on the device and also disables ciphersuites and crypto key configuration.

Syntax

```
ip http secure { server | ciphersuite [rsa-null-md5] [rsa- null-sha] [rsa-des-sha] [rsa-3des-sha] [dh-rsa-des-sha][dh-rsa-3des-sha][rsa-exp1024-des-sha] [rsa-with-aes-128-cbc-sha] [rsa-with-aes-256-cbc-sha] [dhe-rsa-with-aes-128- cbc-sha] [dhe-rsa-with-aes-256-cbc-sha] | crypto key rsa [usage-keys (512|1024|2048|4096)]}
```

```
no ip http secure { server | ciphersuite [rsa-null-md5] [rsa-null-sha] [rsa-des-sha] [rsa-3des-sha] [dh-rsa-des- sha] [dh-rsa-3des-sha] [rsa-exp1024-des-sha] [rsa-with-aes-128-cbc-sha] [rsa-with-aes-256-cbc-sha] [dhe-rsa-with-aes-128-cbc-sha] [dhe-rsa-with-aes-256-cbc-sha]}
```

Parameter

Description

- `server` - Configures the server status to be enabled. When the server status is enabled it establishes the secure layer in the network
- `ciphersuite` - Configures the ciphersuite for providing the input. When an SSL connection is established, the client and server exchange information about which cipher suites they have in common. The options are:
  - `rsa-null-md5` – cipher suites using RSA key exchange. and offering no authentication combined with cipher suites using MD5
  - `rsa-null-sha` – cipher suites using RSA key exchange. and offering no authentication combined with cipher suites using SHA1
  - `rsa-des-sha` – cipher suites using RSA key exchange. and cipher suites using DES, combined with cipher suites using SHA1

- **rsa-3des-sha** – cipher suites using RSA key exchange. and cipher suites using triple DES, combined with cipher suites using SHA1

- **dh-rsa-des-sha** – cipher suites using DH , including anonymous DH with cipher suites using RSA key exchange. and cipher suites using DES, combined with cipher suites using SHA1

- **dh-rsa-3des-sha** – cipher suites using DH , including anonymous DH with cipher suites using RSA key exchange. and cipher suites using triple DES, combined with cipher suites using SHA1

- **rsa-exp-1024-des-sha** – cipher suites using RSA key exchange with export encryption algorithms. Including 40 and 56 bits algorithms and cipher suites using DES, combined with cipher suites using SHA1

- **rsa-with-aes-128-cbc-sha** - cipher suites using RSA key exchange with a 2-bit cipherlist Advanced Encryption Standard (AES algorithms and cipher suites using SHA1

- **rsa-with-aes-256-cbc-sha** - cipher suites using RSA key exchange with a 3-bit cipherlist Advanced Encryption Standard (AES) algorithms and cipher suites using SHA1

- **dhe-rsa-with-aes-128-cbc-sha** - cipher suites using dhe, and cipher suites using RSA key exchange with a 2-bit cipherlist Advanced Encryption Standard (AES) algorithms combined with cipher suites using SHA1

- **dhe-rsa-with-aes-256-cbc-sha** - cipher suites using dhe , and cipher suites using RSA key exchange with a 3-bit cipherlist Advanced Encryption Standard (AES) algorithms combined with cipher suites using SHA1

- **crypto key rsa[usage-keys (512|1024|2048|4096)]** - Configures the usage key (512,1024, 2048 or 4096).

Mode	Global Configuration Mode
Default	ciphersuite - rsa-des-sha:rsa-3des-sha:rsa-exp1024-des-sha:

Example

```
Your Product (config)# ip http secure ciphersuite
rsa-null- sha
```

Related Command(s)

- `show ssl server-cert` - Displays SSL server certificate
- `show ip http secure server status` - Displays SSL status and configuration information

8.2 ssl gen cert-req algo rsa sn

Command Objective	This command creates a request to generate a certificate to the certificate authority. This command uses the RSA key pair and subject name for generating the request. The subject name uniquely identifies the client by the certificate authority
Syntax	`ssl gen cert-req algo rsa sn <SubjectName>`
Mode	Privileged EXEC Mode
Example	`Your Product# ssl gen cert-req algo rsa sn 10.6.4.248`

Related Command(s)

- `show ssl server-cert` - Displays SSL server certificate.
- `show ip http secure server status` - Displays SSL status and configuration information

8.3 ssl server-cert

Command Objective	This command configures the server-certificate input in PEM format. It imports the public certificate of the ssl server. When the ssl server certificate installation is complete, ssl server sends this certificate for authentication of client
Syntax	`ssl server-cert`
Mode	Privileged EXEC Mode
☞	The certificate request must have been created.
Example	`Your Product# ssl server-cert`

Related Command(s)

- `show ssl server-cert` - Displays SSL server certificate
- `show ip http secure server status` - Displays SSL status and configuration information

8.4 debug ssl

Command Objective	This command configures the debug trace messages levels for SSL. System errors such as memory allocation failures are notified using LOG messages and TRACE messages. Interface errors and protocol errors are notified using TRACE messages The no form of the command re-sets the given SSL debug level.

Syntax	`debug ssl ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer])`
	
	`no debug ssl ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer])`

Parameter **Description**	• `all` - Generates debug statements for all traces. • `shut` - Generates debug statements for shutdown traces. This trace is generated on successful shutting down of SSL related module and memory. • `mgmt` - Generates debug statements for management plane functionality traces. • `data` - Generates debug statements for datapath. • `ctrl` - Generates debug statements for Control Plane functionality traces. • `dump` - Generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets. • `resource` - Generates debug statements for Traces with respect to allocation and freeing of all resource except the buffers. • `buffer` - Generates debug statements for traces with respect to allocation and freeing of buffer.
Mode	Privileged EXEC Mode

Default Disabled

Example

```
Your Product# debug ssl all
```

Related Command(s)

- `show ssl server-cert` - Displays SSL server certificate
- `show ip http secure server status` - Displays SSL status and configuration information

8.5 show ssl server-cert

Command Objective	This command displays SSL server certificate information such as Certificate, Data, version, serial number, Signature algorithm.
Syntax	`show ssl server-cert`
Mode	Privileged EXEC Mode
☞	SSL server certificate must have been created.

Example

```
Your Product# show ssl server-cert

Certificate:

Data:

Version: 1 (0x0)

Serial Number: 1 (0x1)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=in, ST=tn, L=ch,
     O=fsoft,OU=ps,
     CN=dheepaag/Email=products@Sup
     ermicro.com

Validity

Not Before: Jan 12 07:40:35 2005 GMT

     Not After: Feb 11 07:40:35 2005

     GMT Subject: CN=dee

Subject Public Key Info:

Public Key Algorithm:rsaEncryption

RSA Public Key:  (1024bit)

     Modulus (1024 bit):

00:b1:cf:8f:04:39:c4:80:bc:f0:2b:40:e0:85:16:
```

```
86:8f:cf:66:84:db:0d:fd:58:d5:fc:12:be:4d:d2:
 e2:ba:d6:d8:95:7c:9d:28:46:45:b3:8a:34:dd:41:
 c2:a3:46:ad:8f:c4:ae:17:37:22:91:c4:0a:8d:79:
 ce:10:34:2c:62:a5:6e:4c:a9:63:2e:93:46:a6:d2:

1c:13:b7:38:02:fb:db:5f:13:46:8e:fb:df:7b:e7:

c8:ba:00:ad:b2:96:cc:1c:4a:8b:2d:51:27:df:eb:

9a:8f:6a:b2:8a:98:92:8e:6a:ed:ba:2e:04:38:3a:

bf:40:f2:d1:37:6c:69:ed:d1

Exponent:65537(0x10001) Signature Algorithm:
 md5WithRSAEncryption

8c:d2:50:01:5c:08:d1:0f:ef:eb:70:56:8e:ea:85:72:32:53:

13:0f:9c:7c:d6:d2:f6:2b:e4:6f:25:4e:86:08:5a:e2:c9:87:

65:cf:98:6c:99:86:a5:55:66:23:b5:b0:f4:56:e6:35:5e:53:

31:00:bc:9f:00:62:34:d1:15:c0:a4:7e:d9:27:c3:d2:d7:01:

13:18:ee:de:f8:52:c8:90:1c:8b:57:15:50:56:8c:b6:7b:4d:

77:e8:23:41:82:dc:9c:47:66:fb:9a:ba:7f:73:a1:d0:88:93:

7b:c3:4b:c8:a5:ec:db:4a:36:19:02:c9:f7:e6:d1:c7:38:d3:

13:f3
```

Related Command(s)

- **`ip http secure`** - Enables SSL server on the device and also configures ciphersuites and crypto keys
- **`ssl gen cert-req algo rsa sn`** - Creates a certificate request using RSA key pair and subjectName
- **`ssl server-cert`** - Configures the server cert, input in PEM format
- **`show ip http secure server status`** - Displays SSL status and configuration information

---

8.6 show ip http secure server status

Command Objective	This command displays SSL status and configuration information. Information such as HTTP secure server status, http secure server ciphersuite are displayed.
Syntax	`show ip http secure server status`
Mode	Privileged EXEC Mode
☞	This command will display output only if http secure server ciphersuite and crypto keys are configured.

Example

```
Your Product# show ip http secure server status

HTTP secure server status: Enabled

HTTP secure server ciphersuite: RSA-DES-SHA:RSA-
3DES- SHA:RSAEXP1024DESSHA:
```

Related Command(s)

- `ip http secure` - Enables SSL server on the device and also configures ciphersuites and crypto keys
- `ssl gen cert-req algorsa sn` - Creates a certificate request using RSA key pair and subjectName
- `ssl server-cert` - Configures the server cert, input in PEM format
- `show ssl server-cert` - Displays SSL server certificate

8.7 version

Command Objective	This command configures the SSL version.
Syntax	`version {all | ssl3 | tls1}`
Parameter Description	• `all` - Allows configuration to both SSL3 and TLS1 SSL protocols. Server accepts all the connection and the https session is established. • `ssl3` - Configures SSL version 3 protocol. • `tls1` - Configures Transport Layer Security version 1 protocol.
Mode	Global Configuration Mode
Default	tls1
Example	`Your Product(config)# version ssl3`
Related Command(s)	• `show ip http secure server status` - Displays SSL status and configuration information

8.8 show restconf status

Command Objective	This command displays the enabled or disabled status of restconf.
Syntax	`show restconf status`
Mode	Privileged EXEC Mode
Example	`Your Product# show restconf status` `Restconf status : Enabled`
Related Command(s)	• `show ip http secure server status` - Displays SSL status and configuration information

8.9 restconf enable

Command Objective	This command enables or disables restconf feature. The default value is enabled
Syntax	`restconf {enable | disable}`
Mode	Global Configuration Mode
Example	`Your Product(config)# restconf disable`
Related Command(s)	• `show ip http secure server status` - Displays SSL status and configuration information

9 SNTP

The SNTP (Simple Network Time Protocol) is a simplified version or subnet of the NTP protocol. It is used to synchronize the time and date in SMIS by contacting the SNTP Server. The administrator can choose whether to set

the system clock manually or to enable SNTP. If SNTP is enabled, the SNTP

implementation discovers the SNTP server and gets the time from the server. The SNTP implementation also has callouts to set the system time based on the time received from the SNTP server. It supports different time zones, where the user can set the required time zone.

The following are the list of SNTP commands:

- `sntp`
- `set sntp client`
- `set sntp client version`
- `set sntp client addressing mode`
- `set sntp client port`
- `set sntp client clock-format`
- `set sntp client time zone`
- `set sntp client clock-summer-time`
- `set sntp client authentication-key`
- `set sntp unicast-server auto-discovery`
- `set sntp unicast-poll-interval`
- `set sntp unicast-max-poll-timeout`
- `set sntp unicast-max-poll-retry`
- `set sntp unicast-server`
- `set sntp broadcast-mode send-request`
- `set sntp broadcast-poll-timeout`
- `set sntp broadcast-delay-time`
- `set sntp multicast-mode send-request`
- `set sntp multicast-poll-timeout`
- `set sntp multicast-delay-time`
- `set sntp multicast-group-address`
- `set sntp manycast-poll-interval`
- `set sntp manycast-poll-timeout`
- `set sntp manycast-poll-retry-count`
- `set sntp manycast-server`
- `show sntp clock`
- `show sntp status`
- `show sntp unicast-mode status`
- `show sntp broadcast-mode status`

- show sntp multicast-mode status
- show sntp manycast-mode status
- debug sntp
- show sntp statistics
- show clock properties
- clock time source
- no clock time source

9.1 sntp

Command Objective	This command enters to SNTP configuration mode which allows the user to execute all the commands that supports SNTP configuration mode.
Syntax	`sntp`
Mode	Global Configuration Mode
Example	`Your Product (config)# sntp` `Your Product (config-sntp)#`

Related Command(s)

- `set sntp client` – Sends the request to the host for time synchronization.
- `set sntp client version` – Sets the operating version of the client SNTP.
- `set sntp client addressing mode` – Sets the addressing mode of SNTP client.
- `set sntp client port`– Sets the listening port for SNTP client which refers to a port on a server that is waiting for a client connection.
- `set sntp client clock format` – Sets the system clock as either AM PM / HOURS format.
- `set sntp client time zone` – Sets the system time zone with respect to UTC.
- `sntp client clock-summer-time`- Enables the DST. (Daylight Saving Time).
- `set sntp client authentication key` - Sets the authentication key for the SNTO clients.
- `set sntp unicast-server auto-discovery` - Configures SNTP client status of auto-discovery

- **set sntp unicast-poll-interval**- Configures SNTP client poll interval.
- **set sntp unicast-max-poll-timeout**- Configures SNTP client maximum poll interval
- **set sntp unicast-max-poll-retry** - Configures SNTP client maximum retry poll count.
- **set sntp unicast-server**- Configures SNTP unicast server.
- **set sntp broadcast-mode send request** - Sets the status of sending the request for knowing the delay.
- **set sntp broadcast-poll-timeout**- Configures SNTP client poll interval in broadcast mode.
- **set sntp broadcast-delay-time**- Configures SNTP delay time in broadcast mode.
- **set sntp multicast-mode send-request** – Sets the status of sending the request for knowing the delay.
- **set sntp multicast-poll-timeout** - Configures SNTP client poll interval in multicast mode.
- **set sntp multicast-delay-time** – set sntp multicast-delay-time - Configures SNTP delay time in multicast mode.
- **set sntp multicast-group-address**- Configures SNTP multicast server address.
- **set sntp manycost-poll-interval**– Configures SNTP client poll interval in manycast mode.
- **set sntp manycast-poll-timeout** – Configures SNTP client poll timeout in manycast mode.
- **set sntp manycast-poll-retry-count** – Configures SNTP poll retries in manycast mode.
- **set sntp manycast-server**- Configures SNTP multicast or broadcast server address in manycast mode.

9.2 set sntp client

Command Objective This command either enables or disables SNTP client module.

Syntax

```
set sntp client {enabled | disabled}
```

Parameter Description

- `enabled` - Enables SNTP client module and sends a request to the host for time synchronization.
- `disabled` - Disables SNTP client module and no request is sent to the host for time synchronization.

Mode SNTP Configuration Mode

Default Disabled.

Example

```
Your Product (config-sntp)# set sntp client enabled
```

Related Command(s)

- `sntp` – Enters to SNTP configuration mode
- `show sntp status` - Displays the status of SNTP client.

9.3 set sntp client version

Command Objective This command sets the operating version of the SNTP for the client.

Syntax

```
set sntp client version { v1 | v2 | v3 | v4 }
```

Parameter Description

- `v1` - Sets the version of SNTP client as 1
- `v2` - Sets the version of SNTP client as 2
- `v3` - Sets the version of SNTP client as 3
- `v4` - Sets the version of SNTP client as 4

Mode SNTP Configuration Mode

Default v4

Example

```
Your Product (config-sntp)# set sntp client version v3
```

Related Command(s)

- `sntp` - Enters to SNTP configuration mode.
- `show sntp status` - Displays the status of SNTP client.

9.4 set sntp client addressing mode

Command Objective This command sets the addressing mode of SNTP client.

Syntax

```
set sntp client addressing-mode { unicast |
broadcast | multicast | manycast }
```

Parameter Description

- `unicast` - Sets the addressing mode of SNTP client as unicast which operates in a point-to-point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally, the round-trip delay and local clock offset relative to the server.
- `broadcast` - Sets the addressing mode of SNTP client as broadcast which operates in a point-to-multipoint fashion. The SNTP server uses an IP local broadcast address instead of a multicast address. The broadcast address is scoped to a single subnet, while a multicast address has Internet wide scope.
- `multicast` - Sets the addressing mode of SNTP client as multicast which operates in point-to-multipoint fashion. The SNTP server uses a multicast group address to send unsolicited SNTP messages to clients. The client listens on this address and sends no requests for updates.
- `manycast` - Sets the addressing mode of SNTP client as manycast which operates in a multipoint-to-point fashion. The SNTP client sends a request to a designated IPv4 or IPv6 local broadcast address or multicast group address. One or more manycast servers reply with their individual unicast addresses.

Mode SNTP Configuration Mode

Default unicast

Example

```
Your Product (config-sntp)# set sntp client
addressing- mode unicast
```

Related Command(s)

- `sntp` - Enters to SNTP configuration mode.
- `show sntp status` - Displays SNTP status.
- `show sntp unicast-mode status` - Displays the SNTP unicast mode status.
- `show sntp broadcast-mode status` – Displays the SNTP broadcast mode status.
- `show sntp multicast-mode status` – Displays the SNTP multicast mode status.
- `show sntp manycast-mode status` – Displays the SNTP manycast mode status.

9.5 set sntp client port

Command Objective	This command sets the listening port for SNTP client which refers to a port on a server that is waiting for a client connection. The value ranges between 1025 and 65535. The no form of this command deletes the listening port for SNTP client and sets the default value.

Syntax	`set sntp client port <portno(1025-65535)>`
	
	`no sntp client port`

Mode	SNTP Configuration Mode
Default	123
☞	This command is executed only if SNTP client is enabled
Example	`Your Product (config-sntp)# set sntp client port 1026`

Related Command(s)

- `sntp` – Enters to SNTP configuration mode.
- `show sntp status` - Displays SNTP status.

9.6 set sntp client clock-format

Command Objective	This command sets the system clock as either AM PM format or HOURS format.
Syntax	`set sntp client clock-format {ampm | hours}`

Parameter Description

- `ampm` - Sets the system clock in am/ pm format
- `hours` - Sets the system clock in 24 hours format

Mode	SNTP Configuration Mode
Default	hours
Example	`Your Product (config-sntp)# set sntp client clock-format ampm`

Related Command(s)

- `sntp` – Enters to SNTP configuration mode.
- `show sntp status` - Displays SNTP status.
- `show sntp clock` - Displays the current time.

9.7 set sntp client time zone

Command Objective	This command sets the system time zone with respect to UTC. The no form of command resets the system time zone to GMT.
Syntax	`set sntp client time-zone <UTC-offset value as (+HH:MM /- HH:MM)(+00:00 to +14:00)/ (-00:00 to -12:00)> Eg: +05:30` `no sntp client time-zone`
Parameter **Description**	• `+/-` - Sets the client time zone as after or before UTC. Plus indicates forward time zone and minus indicates backward time zone. • `UTC-offset value as` - Sets the UTC offset value in hours – `+00:00 to +14:00` – `-00:00 to -12:00`
Mode	SNTP Configuration Mode
Default	+ 00: 00
Example	Your Product (config-sntp)# set sntp client time-zone +05:30
Related Command(s)	• `sntp` – Enters to SNTP configuration mode • `show sntp status` - Displays SNTP status.

9.8 set sntp client clock-summer-time

Command Objective	This command enables the DST (Daylight Saving Time). DST is a system of setting clocks ahead so that both sunrise and sunset occur at a later hour. The effect is additional daylight in the evening. Many countries observe DST, although most have their own rules and regulations for when it begins and ends. The dates of DST may change from year to year. The no form of this command disables the Daylight Saving Time.
Syntax	`set sntp client clock-summer-time <week-day-month,hh:mm><week-day-month,hh:mm> Eg: set sntp client clock-summer-time First-Sun-Mar,05:10 Second-Sun-Nov,06:10 no sntp client clock summer time`
Parameter **Description**	• `week-day-month` – The list is given below; – `week` – First, Second, Third, Fourth or Last week of month. – `day` –Sunday, Monday, Tuesday, Wednesday, Thursday, Friday or Saturday. – `month`: January, February, March, April, May, June, July, August, September, October, November or December. – `hh:mm` - Time in hours and minutes
Mode	SNTP Configuration Mode
Default	Not set

Example

```
Your Product (config-sntp)# set sntp client clock-
summer- time First-Sun-Jan,12:12 Second-Sun-
Mar,12:12
```

Related Command(s)

- `sntp` – Enters to SNTP configuration mode
- `show sntp status` - Displays SNTP status.

9.9 set sntp client authentication-key

Command Objective	This command sets the authentication parameters for the key. Some SNTP severs requires authentication to be done before exchanging any data. This authentication key is used to authenticate the client to the SNTP server to which it tries to connect. The no form of this command disables authentication.
Syntax	`set sntp client authentication-key <key-id> {md5 | des} <key>no sntp client authentication`
Parameter **Description**	• `<key-id>` - Sets a key identifier (integer value) to provide authentication for the server. The value ranges between 1 and 65535. • `md5` - Sets authentication type as md5 where data is verified. MD5 is intended to use with digital signature applications, which requires large files are compressed by a secure method before being encrypted with a secret key, under a public key cryptosystem. • `des` - Sets authentication type as data encryption standard algorithm. • `<key>` - Sets the authentication code as a key value.
Mode	SNTP Configuration Mode
Default	Authentication key ID not set
Example	`Your Product (config-sntp)# set sntp client authentication- key 123 md5 Aricent`

Related Command(s)

- `sntp` – Enters to SNTP configuration mode
- `show sntp status` – Displays SNTP status.

9.10 set sntp unicast-server auto-discovery

Command Objective	This command discovers the entire available SNTP client.
Syntax	`set sntp unicast-server auto-discovery {enabled |disabled}`
Parameter	
Description	• `enabled` - Automatically discovers the entire available SNTP client even if the necessary configuration is not done. • `disabled` - Does not discover any SNTP client.
Mode	SNTP Configuration Mode
Default	Disabled
Example	`Your Product (config-sntp)# set sntp unicast-server auto- discovery enabled`
Related Command(s)	• `sntp` – Enters to SNTP configuration mode. • `Show sntp unicast-mode status` - Displays the SNTP Unicast Mode status.

9.11 set sntp unicast-poll-interval

Command Objective	This command sets the SNTP client poll interval which is the maximum interval between successive messages in seconds. The value ranges between 16 and 16284 seconds.
Syntax	`set sntp unicast-poll-interval <value (16-16284) seconds>`
Mode	SNTP Configuration Mode
Default	64
Example	`Your Product (config-sntp)# set sntp unicast-poll-interval 50`

Related Command(s)

- `sntp` – Enters to SNTP configuration mode.
- `show sntp unicast-mode status` - Displays the SNTP Unicast Mode status.

9.12 set sntp unicast-max-poll-timeout

Command Objective	This command configures SNTP client maximum poll interval timeout which is the maximum interval to wait for the poll to complete. The value ranges between 1 and 30 in seconds.
Syntax	`set sntp unicast-max-poll-timeout <value (1-30) seconds>`
Mode	SNTP Configuration Mode
Default	5
Example	`Your Product (config-sntp)# set sntp unicast-max-poll- timeout 25`

Related Command(s)

- `sntp` – Enters to SNTP configuration mode.
- `show sntp unicast-mode status` - Displays the SNTP Unicast Mode status.

9.13 set sntp unicast-max-poll-retry

Command Objective	This command configures SNTP client maximum retry poll count which is the maximum number of unanswered polls that cause a slave to identify the server as dead. The value ranges between 1 and 10 in times.
Syntax	`set sntp unicast-max-poll-retry <value (1-10) times>`
Mode	SNTP Configuration Mode
Default	3
Example	`Your Product (config-sntp)# set sntp unicast-max-poll- retry 10`
Related Command(s)	• `sntp` – Enters to SNTP configuration mode • `show sntp unicast-mode status` - Displays the SNTP Unicast Mode status.

9.14 set sntp unicast-server

Command Objective	This command configures SNTP unicast server. The no form of this command deletes the sntp unicast server attributes and sets to default value.
Syntax	`set sntp unicast-server {ipv4 <ucast_addr> | ipv6 <ip6_addr> | domain-name <string(64)>} [{primary | secondary}] [version {3 | 4 }] [port <integer(1025-36564)>]` `no sntp unicast-server {ipv4 <ucast_addr> | ipv6 <ip6_addr> | domain-name <string(64)> }`
Parameter	
Description	• `ipv4 <ucast_addr>` - Sets the address type of the unicast server as Internet Protocol Version 4. • `ipv6 <ip6_addr>` - Sets the address type of the unicast server as • Internet Protocol Version 6. • `domain-name <string(64)>` - Sets the domain name for the unicast server. This value is a string with the maximum size as 64. • `primary` - Sets the unicast server type as primary server. • `secondary` - Sets the unicast server type as secondary server. • `version 3` - Sets the SNTP version as 3. • `version 4` - Sets the SNTP version as 4. • `port <integer(1025-36564)>` - Selects the port identifier numbers in the selected server. This value ranges between 1025 and 36564.
Mode	SNTP Configuration Mode
Default	version 4

Example

```
Your Product (config-sntp)# set sntp unicast-server
ipv4 12.0.0.100 Primary version 3 port 1234
```

Related Command(s)

- `sntp` – Enters to SNTP configuration mode
- `show sntp unicast-mode status` - Displays the SNTP Unicast Mode status.
- `show sntp status` – Displays SNTP status.

9.15 set sntp broadcast-mode send-request

Command Objective	This command either enables or disables the sntp to send status request.
Syntax	`set sntp broadcast-mode send-request {enabled | disabled}`
Parameter Description	• `enabled` - Sends the SNTP request packet to broadcast server to calculate the actual delay. • `disabled` - Does not send any SNTP request packet to broadcast server instead default value for the delay is taken.
Mode	SNTP Configuration Mode
Default	disabled
Example	`Your Product (config-sntp)# set sntp broadcast-mode send- request enabled`
Related Command(s)	• `sntp` – Enters to SNTP configuration mode • `show sntp broadcast-mode status` – Displays the SNTP broadcast mode status.

9.16 set sntp broadcast-poll-timeout

Command Objective	This command configures SNTP client poll interval in broadcast mode which is the maximum interval to wait for a poll to complete. The value ranges between 1 and 30 seconds.
Syntax	`set sntp broadcast-poll-timeout [<value (1-30) seconds>]`
Mode	SNTP Configuration Mode
Default	5
Example	`Your Product (config-sntp)# set sntp broadcast-poll-timeout 30`

Related Command(s)

- `sntp` - Enters to SNTP configuration mode
- `show sntp broadcast-mode status` – Displays the SNTP broadcast mode status

9.17 set sntp broadcast-delay-time

Command Objective	This command configures SNTP delay time in broadcast mode which is the time interval the SNTP client needs to wait for a response from the server. The value ranges between 1000 and 15000 in microseconds.
Syntax	`set sntp broadcast-delay-time [<value (1000-15000) microseconds>]`
Mode	SNTP Configuration Mode
Default	8000
Example	`Your Product (config-sntp)# set sntp broadcast-delay-time 2000`
Related Command(s)	• `sntp` – Enters to SNTP configuration mode • `show sntp broadcast-mode status` – Displays the SNTP broadcast mode status

9.18 set sntp multicast-mode send-request

Command Objective	This command sets the status of sending the request to the multicast server to calculate the delay time.
Syntax	`set sntp multicast-mode send-request {enabled | disabled}`
Parameter	
Description	• `enabled` - Sends the SNTP request to the multicast server to calculate the actual delay time. • `disabled` - Does not send any SNTP request to the multicast server.
Mode	SNTP Configuration Mode
Default	Disabled
Example	`Your Product (config-sntp)# set sntp multicast-mode send- request enabled`
Related Command(s)	• `sntp` – Enters to SNTP configuration mode • `show sntp multicast-mode status` – Displays the SNTP multicast mode status

9.19 set sntp multicast-poll-timeout

Command Objective	This command configures SNTP client poll interval in multicast mode which is the maximum interval to wait for the poll to complete. The value ranges between 1 and 30 seconds.
Syntax	`set sntp multicast-poll-timeout [<value (1-30) seconds>]`
Mode	SNTP Configuration Mode
Default	5
Example	`Your Product (config-sntp)# set sntp multicast-poll- timeout 10`

Related Command(s)

- `sntp` – Enters to SNTP configuration mode.
- `show sntp multicast-mode status` – Displays the SNTP multicast mode status.

9.20 set sntp multicast-delay-time

Command Objective	This command configures SNTP delay time in which there is no response from the multicast server. The value ranges between 1000 and 15000 in microseconds.
Syntax	`set sntp multicast-delay-time [<value (1000-15000) microseconds>]`
Mode	SNTP Configuration Mode
Default	8000
Example	`Your Product (config-sntp)# set sntp multicast-delay-time 2000`
Related Command(s)	• `sntp` – Enters to SNTP configuration mode • `show sntp multicast-mode status` – Displays the SNTP multicast mode status

9.21 set sntp multicast-group-address

Command Objective	This command configures a group address for the SNTP so that all the SNTP client servers can be connected to this address.
Syntax	`set sntp multicast-group-address {ipv4 {<mcast_addr> | default} | ipv6 {<ipv6_addr> | default}}`
Parameter	
Description	• `ipv4` - Sets the Internet Protocol Version as version 4 – `<mcast_addr>` - Sets the multicast group address – `default` – Sets the multicast default address as a default value • `ipv6` - Sets the Internet Protocol Version as version 6 – `< ipv6_addr >` - Sets the ipv6 address – `default` – Sets the multicast default address as a default value
Mode	SNTP Configuration Mode
Example	`Your Product (config-sntp)# set sntp multicast-group- address ipv4 224.1.1.10`
Related Command(s)	• `sntp` – Enters to SNTP configuration mode. • `show sntp multicast-mode status` – Displays the SNTP multicast mode status.

9.22 set sntp manycast-poll-interval

Command Objective	This command configures SNTP client poll interval which is the maximum interval between successive messages. The poll interval value ranges between 60 and 16284 in seconds.
Syntax	`set sntp manycast-poll-interval [<value (60-16284) seconds>]`
Mode	SNTP Configuration Mode
Default	64
Example	`Your Product (config-sntp)# set sntp manycast-poll-interval 60`

Related Command(s)

- `sntp` – Enters to SNTP configuration mode.
- `set sntp client addressing-mode` – Sets the addressing mode of SNTP.
- `show sntp manycast-mode status` – Displays the SNTP manycast mode status.

9.23 set sntp manycast-poll-timeout

Command Objective	This command configures SNTP client poll timeout which is the maximum interval to wait for a poll to complete. The value ranges between 1 and 30 in seconds.
Syntax	`set sntp manycast-poll-timeout [<value (1-30) seconds>]`
Mode	SNTP Configuration Mode
Default	5
Example	`Your Product (config-sntp)# set sntp manycast-poll-timeout 10`

Related Command(s)

- `sntp` – Enters to SNTP configuration mode.
- `set sntp client addressing-mode` – Sets the addressing mode of SNTP
- `show sntp manycast-mode status` – Displays the SNTP manycast mode status.

9.24 set sntp manycast-poll-retry-count

Command Objective	This command configures SNTP poll retries count which is the maximum number of unanswered polls that cause a slave to identify the server as dead. The value ranges between 1 and 10 in seconds.
Syntax	`set sntp manycast-poll-retry-count [<value (1-10)>]`
Mode	SNTP Configuration Mode
Default	3
Example	`Your Product (config-sntp)# set sntp manycast-poll-retry- count 5`
Related Command(s)	• `sntp` – Enters to SNTP configuration mode. • `set sntp client addressing-mode` – Sets the addressing mode of SNTP • `show sntp manycast-mode status` – Displays the SNTP manycast mode status

9.25 set sntp manycast-server

Command Objective	This command configures SNTP multicast or broadcast server address in manycast mode.
Syntax	`set sntp manycast-server { broadcast | multicast {ipv4 [<mcast_addr>] |ipv6 [<ip6_addr>]} }`
Parameter Description	• `broadcast` - Configures SNTP broadcast server address in manycast mode • `multicast` - Configures SNTP multicast server address in manycast mode. • `ipv4 < mcast_addr>` - Sets the multicast server address in internet protocol v4. • `ipv6 <ipv6_addr>` - Sets the multicast server address in internet protocol v6.
Mode	SNTP Configuration Mode
Example	`Your Product (config-sntp)# set sntp manycast-server multicast ipv4 224.0.0.1`
Related Command(s)	• `sntp` – Enters to SNTP configuration mode • `show sntp manycast-mode status` – Displays the SNTP manycast mode status

9.26 show sntp clock

Command Objective	This command displays the current time.
Syntax	`show sntp clock`
Mode	User / Privileged EXEC Mode
Example	`Your Product# show sntp clock` `current time : Sat Jan 01 2000 21:41:30 (UTC +00:00 )`
Related Command(s)	• `set sntp client clock-format` - Sets the system clock as either AM PM format or HOURS format.

9.27 show sntp status

Command Objective	This command displays SNTP status.
Syntax	`show sntp status`
Mode	User / Privileged EXEC Mode

Example

```
Your Product# show sntp status
sntp client is enabled
current sntp client version is v4
current sntp client addressing mode is
 unicast sntp client port is 123
sntp client clock format is 24 hours sntp client
 authenticatin key id is 5
sntp client authentication algorithm is md5
sntp client auth Key is
 Aricent sntp client time
 zone is  + 05:30
sntp client dst start time is not set
sntp client dst end time is not set
```

Related Command(s)

- `set sntp client` – Sends the request to the host for time synchronization.
- `set sntp client version` – Sets the operating version of the client SNTP.
- `set sntp client addressing mode` – Sets the addressing mode of SNTP client.

- **set sntp client port** – Sets the listening port for SNTP client which refers to a port on a server that is waiting for a client connection.
- **set sntp client clock-format** – Sets the system clock as either AM PM / HOURS format.
- **set sntp client authentication-key** – Sets the authentication key for the SNTO clients.
- **set sntp client time-zone** – Sets the system time zone with respect to UTC.
- **sntp client clock-summer-time** – Enables the Daylight Saving Time.
- **show sntp unicast-mode status** – Displays the SNTP Unicast Mode status.
- **show sntp broadcast-mode status** – Displays the SNTP broadcast mode status
- **show sntp multicast-mode status** - Displays the SNTP multicast mode status
- **show sntp manycast-mode status** - Displays the SNTP manycast mode status

9.28 show sntp unicast-mode status

Command Objective	This command displays the status of SNTP in unicast mode.
Syntax	`show sntp unicast-mode status`
Mode	User / Privileged EXEC Mode
☞	This command is executed only if the addressing mode is set as unicast.

Example

```
Your Product# show sntp unicast-mode status

auto discovery of sntp/ntp servers is disabled
 unicast poll interval value is 64

unicast max poll time out value is 5 unicast max
 retry time value is 3

Unicast current mode value is NOT SYNCHRONIZED

Sntp client is up for 00:03:22

unicast primary server address is
 12.0.0.1 unicast primary server
 version is 4 unicast primary
 server port is 1056
```

Related Command(s)

- `set sntp client addressing mode` – Sets the addressing mode of SNTP client.
- `set sntp unicast-server auto-discovery` - Configures SNTP client status of auto-discovery of server.
- `set sntp unicast-poll-interval` - Configures SNTP client poll interval.

- **Set sntp unicast-max-poll-timeout** - Configures SNTP client maximum poll interval timeout.
- **set sntp unicast-max-poll-retry** - Configures SNTP client maximum retry poll count.
- **set sntp unicast-server** - Configures SNTP unicast server.
- **show sntp status** - Displays the status of SNTP client.

9.29 show sntp broadcast-mode status

Command Objective	This command displays the status of SNTP in broadcast mode.
Syntax	`show sntp broadcast-mode status`
Mode	User / Privileged EXEC Mode
☞	This command is executed only if the addressing mode is set as broadcast.

Example	`Your Product# show sntp broadcast-mode status`
	`send sntp request to server in broadcast mode is disabled broadcast poll time out value is 5`
	`broadcast delay time value is 8000`
	`broadcast sntp server is 12.0.0.100`

Related Command(s)	• `set sntp client addressing mode` – Sets the addressing mode of SNTP client. • `set sntp broadcast-mode send-request` - Sets the status of sending the request for knowing the delay. • `set sntp broadcast-poll-timeout` - Configures SNTP client poll interval in broadcast mode. • `set sntp broadcast-delay-time` - Configures SNTP delay time in broadcast mode. • `Show sntp status`- Displays the status of SNTP client.

9.30 show sntp multicast–mode status

Command Objective	This command displays the status of SNTP in multicast mode.
Syntax	`show sntp multicast-mode status`
Mode	User / Privileged EXEC Mode
☞	If command is executed only if the SNTP client addressing mode is set as multicast.

Example

```
Your Product# show sntp multicast-mode status
send sntp request to server in multicast mode is
disabled multicast poll time out value is 5
multicast delay time value is 8000
multicast group address is 12.0.0.100
```

Related Command(s)

- `set sntp client addressing mode` – Sets the addressing mode of SNTP client.
- `set sntp multicast-mode send-request` - Sets the status of sending the request for knowing the delay.
- `set sntp multicast-poll-timeout` - Configures SNTP client poll interval in multicast mode.
- `set sntp multicast-delay-time` - Configures SNTP delay time in multicast mode.
- `set snto multicast-group-address` - Configures SNTP multicast server address.
- `show sntp status`- Displays the status of SNTP client.

9.31 show sntp manycast-mode status

Command Objective	This command displays the SNTP manycast mode status.
Syntax	`show sntp manycast-mode status`
Mode	User / Privileged EXEC Mode
☞	This command executes only if the SNTP client addressing mode is set as manycast.
Example	**`Your Product# show sntp manycast-mode status`** `manycast poll interval value is 64 manycast max poll time out value is 5 manycast max retry time value is 3 manycast server type is broadcast primary server address is 12.0.0.100`

Related Command(s)

- `set sntp client addressing mode` – Sets the addressing mode of SNTP client.
- `set sntp manycast-poll-interval` - Configures SNTP client poll interval in manycast mode.
- `set sntp manycast-poll-timeout` - Configures SNTP client poll timeout in manycast mode.
- `set sntp manycast-poll-retry-count` - Configures SNTP poll retries in manycast mode.
- `set sntp manycast-server`- Configures SNTP multicast or broadcast server address in manycast mode.
- `show sntp status`- Displays the status of SNTP client.

9.32 debug sntp

Command Objective

This command enables SNTP trace.

The no form of the command disables the SNTP trace.

Syntax

```
debug sntp {all | [init-shut] [mgmt] [data-path]
[control] [pkt-dump] [resource] [all-fail] [buff]}

no debug sntp {all | [init-shut] [mgmt]
[data-path] [control] [pkt-dump] [resource]
[all-fail] [buff]}
```

Parameter Description

- `all` - Generates debug statements for all kinds of traces
- `init-shut` - Generates debug statements for init and shutdown traces.
- This trace is generated on failed initialization and shutting down of SNTP related entries
- `mgmt` - Generates debug statements for management traces. This trace is generated during failure in configuration of any of the SNTP features.
- `data-path` - Generates debug statements for data path traces. This trace is generated during failure in packet processing.
- `control` - Generates debug statements for control path traces. This trace is generated during failure in modification or retrieving of SNTP entries.
- `pkt-dump` - Generates debug statements for packet dump traces. This trace is currently not used in SNTP module.
- `resource` - Generates debug statements for OS resource related traces. This trace is generated during failure in message queues.
- `all-fail` - Generates debug statements for all failure traces of the above-mentioned traces.
- `buff` - Generates debug statements for SNTP buffer related traces. This trace is currently not used in SNTP module.

Mode

User / Privileged EXEC

Mode Default	Debugging is Disabled
Example	`debug sntp all`

9.33 show sntp statistics

Command Objective	This command displays the sntp packet statistics.
Syntax	`show sntp statistics`
Mode	User / Privilege EXEC Mode

Example	`Your Product# show sntp statistics`
	`Number of SNTP server-reply Received: 0`
	`Number of SNTP client-request Transmitted: 0`
	`Number of SNTP Pkt InDiscards: 0`

9.34 show clock properties

Command Objective This command displays primary system clock properties.

Syntax `show clock properties`

Mode User / Privilege EXEC Mode

☞ Now only the clock sourec is meaningful.

Example

```
Your Product# show clock properties

SMIS# show clock properties

System Clock Information

------------------------

Variance: 0

Class: 248

Accuracy: Unknown

Source: CMM

Offset: 0 (UTC)

HoldOver: Enabled

Clock in sync with time source
```

Related Command(s)

- `clock time source` – Configure the time source of primary clock.
- `no clock time source` - Reset time source of the primary clock to default time source.

9.35 clock time source

Command Objective This command is to configure the time source of primary clock.

Syntax

```
clock time source { atomic-clock | gps |  ptp | ntp
 | cmm | internal-oscillator}
```

Mode Privilege EXEC Mode

☞ Now only ntp and cmm clock source are applicable.

Example

```
Your Product# clock time source ntp
```

Description

- `atomic-clock` - Primary time source of the system is atomic-clock
- `gps` - Primary time source of the system is gps.
- `ptp` - Primary time source of the system is ptp.
- `ntp` - Primary time source of the system is ntp.
- `cmm` - Primary time source of the system is cmm.
- `internal-oscillator` - Primary time source of the system is internal-oscillator

Related Command(s)

- `show clock properities` – Displays primary system clock properties.
- `no clock time source` - Reset time source of the primary clock to default time source

9.36 no clock time source

Command Objective	Reset time source of the primary clock to default time source
Syntax	`no clock time source`
Mode	Privilege EXEC Mode
Default	Default time source is cmm
Example	`Your Product# no clock time source`

Related Command(s)

- `show clock properities` – Displays primary system clock properties
- `clock time source` - Configure the time source of primary clock

10 SNMPv3

SNMP (Simple Network Management Protocol) is the most widely-used network management protocol on TCP/IP-based networks. SNMPv3 is designed mainly to overcome the security shortcomings of SNMPv1/v2. USM (User based Security Model) and VACM (View based Access Control Model) are the main features added as part of the SNMPv3 specification. USM provides both encryption and authentication of the SNMP PDUs, while VACM specifies a mechanism for defining access policies for different users with different MIB trees. Also, SNMPv3 specifies a generic management framework, which is expandable for adding new Management Engines, Security Models, Access Control Models and so on. With SNMPv3, the SNMP communication is completely safe and secure.

The list of CLI commands for the configuration of SNMPv3 is as follows:

- `enable snmpsubagent`
- `disable snmpsubagent`
- `enable snmpagent`
- `disable snmpagent`
- `snmp community index`
- `snmp group`
- `snmp access`
- `snmp engineid`
- `snmp proxy name`
- `snmp mibproxy name`
- `snmp view`
- `snmp targetaddr`
- `snmp targetparams`
- `snmp user`
- `snmp notify`
- `snmp filterprofile`
- `snmp-server enable traps snmp authentication`
- `snmp-server trap udp-port`
- `snmp-server trap proxy-udp-port`
- `snmp agent port`
- `snmp tcp enable`
- `snmp trap tcp enable`
- `snmp-server tcp-port`
- `snmp-server trap tcp-port`
- `snmp-server enable traps`
- `show snmp agentx information`
- `show snmp agentx statistics`
- `show snmp`
- `show snmp community`

- show snmp group
- show snmp group access
- show snmp engineID
- show snmp proxy
- show snmp mibproxy
- show snmp viewtree
- show snmp targetaddr
- show snmp targetparam
- show snmp user
- show snmp notif
- show snmp inform statistics
- show snmp-server traps
- show snmp-server proxy-udp-port
- show snmp tcp
- show snmp filter
- snmpset mib
- snmpget mib
- snmpgetnext mib
- snmpwalk mib
- snmp filter trap
- show mib oid
- show mib name

10.1 enable snmpsubagent

Command Objective

This command configures the SNMP to act as a snmp agentx-subagent and also configures the master agent parameters

Syntax

```
enable snmpsubagent { master { ip4 <ipv4_address> |
ip6<ipv6_address> } [port <number>] }
```

Parameter Description

- `master` - Registers all the master agent information and agent capabilities after successful index allocation.
- `ip4<ipv4_address>` - Configures the ip address of the master agent with the given v4 IP address.
- `ip6<ipv6_address>` - Configures the ip address of the master agent with the given v6 IP address.
- `port<number>` - Sets the master port number through which the Agentx PDUs are transmitted to the master agent.

Mode

Global Configuration Mode

Default

port - 705

☞ This Example is executable only if snmp agent is disabled.

Example

```
Your Product (config)# enable snmpsubagent master ip4
10.0.0.5 port 897
```

Related Command(s)

- `disable snmpsubagent` – Disables agentx-subagent

- `disable snmpagent` – Disables SNMP agent.
- `enable snmpagent` – Enables SNMP agent.
- `show snmp agentx information` – Displays global information of SNMP Agentx communications.
- `show snmp agentx statistics` – Displays all the information regarding SNMP Agentx statistics.

10.2 disable snmpsubagent

Command Objective	This command disables agentx-subagent.
Syntax	`disable snmpsubagent`
Mode	Global Configuration Mode
Example	`Your Product (config)# disable snmpsubagent`

Related Command(s)

- `enable snmpsubagent` - Enables agentx-subagent capabilities.
- `show snmp agentx information` – Displays global information of SNMP Agentx communications.
- `show snmp agentx statistics`– Displays all the information regarding SNMP Agentx statistics.

10.3 enable snmpagent

Command Objective	This command enables SNMP agent which provides an interface between a SNMP manager and a switch. The agent processes SNMP packets received from the manager, frames the appropriate response packets and sends them to the manager.
Syntax	`enable snmpagent`
Mode	Global Configuration Mode
Default	SNMP agent is enabled.
Example	`Your Product (config)# enable snmpagent`

Related Command(s)

- `enable snmpsubagent` - Enables agentx-subagent capabilities.
- `disable snmpagent` - Disables SNMP agent.

10.4 disable snmpagent

Command Objective	This command disables SNMP agent.
Syntax	`disable snmpagent`
Mode	Global Configuration Mode
Example	`Your Product (config)# disable snmpagent`

Related Command(s)

- `enable snmosubagent` - Enables either snmp agent or agentx-subagent capabilities.
- `enable snmpagent` – Enables SNMP agent.
- `show snmp agentx statistics` – Displays all the information regarding SNMP Agentx statistics.

10.5 snmp community index

Command Objective

This command configures the SNMP community details.

The no form of this command removes the SNMP community details.

Syntax

```
snmp community index <CommunityIndex> name
<CommunityName> security <SecurityName> [context
  <Name >]
[{volatile | nonvolatile}] [transporttag
<TransportTagIdentifier | none>] [contextengineid
<ContextEngineID>]
no snmp community index <CommunityIndex>
```

Parameter

Description

- `<CommunityIndex>` - Creates a community index identifier which stores the index value of the row. This ID must be unique for every community name entry.
- `name<CommunityName>` - Creates a community name which stores the community string.
- `security<SecurityName>` - Stores the security model of the corresponding Snmp community name.
- `Context <Name>` - Indicates the name of the context in which the management information is accessed when using the community string specified by the corresponding instance of snmp community name
- `volatile | nonvolatile` - Sets the storage type as either volatile or non volatile.
- `volatile` – Sets the storage type as temporary and erases the configuration setting on restarting the system.
- `nonvolatile` – Sets the storage type as permanent and saves the configuration to the system. The saved configuration can be viewed on restarting the system.

- **<TransportTagIdentifier>** - Specifies a set of transport endpoints from which a command responder application can accept management request.
- **contextengineid<ContextEngineID>** - Indicates the location of the context through which the management information is accessed when using the community string specified by the corresponding instance of snmp community name

---

Mode

Global Configuration Mode

Default

- Community Index - NETMAN/PUBLIC
- CommunityName - NETMAN/PUBLIC
- Security Name – None
- ContextName – Null
- Context EngineID - 80.00.08.1c.04.46.53
- Transport Tag – Null
- Storage type - Non Volatile
- Row Status - Active

Example

```
Your Product (config)# snmp community index
myv3com name myv3com security xyz context myinst
nonvolatile transporttag myv3tag
```

Related Command(s)

- **show snmp** - Displays the status information of SNMP communications
- **show snmp community** - Displays the configured SNMP community details

---

10.6 snmp group

Command Objective

This command configures SNMP group details.

The no form of the command removes the SNMP group details.

Syntax

```
snmp group <GroupName> user <UserName> security-model
{v1| v2c | v3 } [{volatile | nonvolatile}]

no snmp group <GroupName> user <UserName> security-
model{v1 | v2c | v3 }
```

Parameter

Description

- `<GroupName>` - Creates a name for an SNMP group
- `user<UserName>` - Sets a user for the configured group.
- `security-model` - Sets the security model for SNMP
- `v1` - Sets the SNMP version as Version 1.
- `v2c` - Sets the SNMP version as Version 2.
- `v3` - Sets the SNMP version as Version 3.
- `volatile | nonvolatile` - Sets the required storage type for the group entry
- `volatile` – Sets the storage type as temporary. Erases the configuration setting on restarting the system.
- `nonvolatile` – Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.

Mode

Global Configuration Mode

Default

- Security model - V3
- Security Name - none / initial / templateMD5 / templateSHA
- Group Name - iso/initial
- Storage Type - non volatile

- Row status - Active

Example

```
Your Product (config)# snmp group myv3group user
myv3user security-model v1 volatile
```

Related Command(s)

- `snmp access` - Configures the SNMP group access details
- `show snmp group` - Displays the configured SNMP groups
- `show snmp user` - Displays the configured SNMP users
- `show snmp group` – Displays the configured SNMP groups.

10.7 snmp access

Command Objective

This command configures the SNMP group access details. To configure an SNMP access along with the group, a group must have already been created using the snmp group command.

The no form of the command removes the SNMP group access details.

Syntax

```
snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}} [read <ReadView | none>] [write <WriteView | none>] [notify <NotifyView | none>] [{volatile | nonvolatile}] [context <string(32)> ]

no snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}}
```

Parameter

Description

- `<GroupName>` - Sets the name of the group for which access is to be provided.
- `v1 | v2c | v3-` Sets the SNMP verison.
  - `v1` – Sets the SNMP version as Version 1.
  - `v2c` – Sets the SNMP version as Version 2.
  - `v3` – Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word
- `auth` - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication.
- `noauth` - Sets no-authentication
- `priv` - Sets both authentication and privacy
- `read` - Mentions the MIB view of the SNMP context to which read access is authorized by this entry
- `write` - Mentions the MIB view of the SNMP context to which write access is authorized by this entry
- `notify` - Mentions the MIB view of the SNMP context to which notification access is authorized by this entry
- `volatile | nonvolatile` - Sets the required storage type for the group entry
  - `volatile` – Sets the storage type as temporary. Erases the configuration setting on restarting the system.

- **nonvolatile** – Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.

- **context<string(32)>** - Configures the name of the SNMP context. The maximum length of the string is 32.

Mode

Global Configuration Mode

Default

- Group Name - iso
- Read/Write/Notify view - iso
- Storage Type - volatile
- Row status - Active
- Group Name - initial
- Read/Write/Notify View - restricted
- Storage Type - non-volatile
- Group Name - Initial
- Read/Write/Notify View - iso
- Storage Type - non-volatile

Example

```
Your Product (config)# snmp access myv2group
v2 read v2readview write v2writeview notify
v2notifyview nonvolatile
```

Related Command(s)

- **snmp group** - Configures SNMP group details
- **snmp view** - Configures the SNMP view
- **show snmp group** - Displays the configured SNMP groups
- **show snmp group access** - Displays the configured SNMP group access details
- **show snmp viewtree** - Displays the configured SNMP Tree views

---

10.8 snmp engineid

Command Objective

This command configures the engine ID that is utilized as a unique identifier of a SNMPv3 engine. This engine ID is used to identify a source SNMPv3 entity and a destination SNMPv3 entity to coordinate the exchange of messages between the source and the destination.

The no form of the command resets the engine ID to the default value.

Syntax

```
snmp engineid <EngineIdentifier>

no snmp engineid
```

Mode

Global Configuration Mode

Default

80.00.08.1c.04.46.53

- The Engine ID must be given as octets in hexadecimal separated by dots and the allowed length is 5 to 32 octets.
- SNMP engine ID is an administratively unique identifier.
- Changing the value of the SNMP engine ID has significant effects.
- All the user information will be updated automatically to reflect the change

Example

```
Your Product (config)# snmp engineid
80.0.08.1c.04.5f.a9
```

Related Command(s)

- `show snmp engineID` - Displays the Engine Identifier
- `show snmp user` - Displays the configured SNMP users

10.9 snmp proxy name

Command Objective

This command configures the proxy.

The no form of the command removes the proxy.

Syntax

```
snmp proxy name <ProxyName> ProxyType {Read | Write |
inform | Trap} ContextEngineID <EngineId>
TargetParamsIn
<TargetParam> TargetOut <TargetOut> [ContextName
<ProxyContextName>] [StorageType {volatile |
nonvolatile}]
no snmp proxy name <ProxyName>
```

Parameter Description

- `<ProxyName>` - Identifies an entry in the proxy table.

This will be the INDEX used for the Proxy Table.

- `ProxyType` - Forwards the messages using the translation parameters defined by proxy entry. The options are:
  - `Read` – Forwards the read messages to get the request from the manager.
  - `Write` – Forwards the write messages to set configurations.
  - `Inform` – Forwards the notification messages to the agent.
  - `Trap` – Forwards the SNMP trap messages to the agent
- `ContextEngineID <EngineId>` - Configures a context engine ID of the agent with whom the manager communicates through the proxy.
- `TargetParamsIn <TargetParam>` - Configures the SNMP version that the manager sends as request to the proxy.
- `TargetOut <TargetOut>` - Configures the SNMP version that the proxy uses to communicate with multiple agent.

This object is only used when selection of a single target is required (that is, when forwarding an incoming read or write request).

- **ContextName <ProxyContextName>** - Configures a unique context name for an SNMP sub agent. This name is used to identify the corresponding sub agent when more than one sub agent exists.
- **Storage Type** - Sets the required storage type for the group entry

  – **volatile** – Sets the storage type as temporary. Erases the configuration setting on restarting the system.

  – **nonvolatile** – Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.

Mode Global Configuration Mode

Default Storage Type - Nonvolatile

Example

```
Your Product (config)# snmp proxy name proxy1
ProxyType write ContextEngineID
80.00.08.1c.04.46.53 TargetParamsIn param2
TargetOut target2  ContextName pxyctxtname
StorageType nonvolatile
```

Related Command(s)

- **show snmp group** - Displays the configured SNMP groups
- **show snmp proxy** – Displays proxy details.

10.10 snmp mibproxy name

Command Objective	This command configures the mib proxy. The no form of the command removes the mib proxy.

Syntax

```
snmp mibproxy name <ProxyName> ProxyType {Read |
Write | inform | Trap} mibid <MibId>
TargetParamsIn <TargetParam> TargetOut
<TargetOut> [StorageType {volatile |
nonvolatile}]

no snmp mibproxy name <ProxyMibName>
```

Parameter

Description

- `<ProxyName>` - Identifies an entry in the proxy table

This will be the INDEX used for the Proxy Table.

- `ProxyType` - Forwards the messages using the translation parameters defined by proxy entry. The list contains: Options are:

– `Read` – Forwards the read messages to get the request from the manager.

– `Write` – Forwards the write messages to set configurations.

– `Inform` – Forwards the notification messages to the agent.

– `Trap` – Forwards the SNMP trap messages to the agent

- `Mibid <MibId>` - Configures a context MIB ID of the agent with whom the manager communicates through the proxy.
- `TargetParamsIn<TargetParam>` - Configures the SNMP version that the manager sends as request to the proxy.
- `TargetOut<TargetOut>` - Configures the SNMP version that the proxy uses to communicate with multiple agent. This object is only used when selection of a single target is required (that is, when forwarding an incoming read or write request).
- `Storage Type` - Storage type. Options are:

– **volatile** – Sets the storage type as temporary. Erases the configuration setting on restarting the system.

– **nonvolatile** – Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.

Mode Global Configuration Mode

Example

```
Your Product (config)# snmp mibproxy name mibproxy1

ProxyType read mibid 1 TargetParamsIn param1
TargetOut target1 StorageType nonvolatile
```

Related Command(s)

- **show snmp group** - Displays the configured SNMP groups
- **show snmp mibproxy** - Displays the mib proxy details.

10.11 snmp view

Command Objective

This command configures the SNMP view.

The no form of the command removes the SNMP view.

Syntax

```
snmp view <ViewName> <OIDTree> [mask <OIDMask>]
{included | excluded} [{volatile | nonvolatile}]

no snmp view <ViewName> <OIDTree>
```

Parameter

Description

- `<ViewName>` - Specifies the view name for which the view details are to be configured. This is a string value with maximum size as 32.
- `<OIDTree>` - Specifies the sub tree value for the particular view.
- `mask <OIDMask>` - Specifies a mask value for the particular view.
- `included` - Allows access to the subtree
- `excluded` - Denies access to the subtree
- `volatile` - Sets the storage type as temporary. Erases the configuration setting on restarting the system.
- `nonvolatile` - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration can be viewed on restarting the system.

Mode

Global Configuration Mode

Default

- View Name - iso/restricted
- OIDTree - 1
- OIDMask - 1
- View type - included
- Storage type - non-volatile
- Row status - Active

☞ To configure an SNMP view (read/write/notify), a group must have already been created using the **snmp group**command and SNMP group access must be configured using the **snmp access**command.

Example

```
Your Product (config)# snmp view v2readview 1.3.6.1
mask 1.1.1.1 included nonvolatile
```

Related Command(s)

- `snmp access` - Configures the SNMP group access details
- `show snmp viewtree` - Displays the configured SNMP Tree views
- `show snmp group access` - Displays the configured SNMP group access details

10.12 snmp targetaddr

Command Objective

This command configures the SNMP target address.

The no form of the command removes the configured SNMP target address.

Syntax

```
snmp targetaddr <TargetAddressName> param <ParamName>
{<IPAddress> | <IP6Address>} [timeout <Seconds(1-1500>]
[retries <RetryCount(1-3)] [taglist <TagIdentifier | none>] [{volatile | nonvolatile}] [port <integer (1-65535)>]
no snmp targetaddr <TargetAddressName>
```

Parameter Description

- `<TargetAddressName>` - Configures a unique identifier of the Target.
- `param<ParamName>` - Configures the parameters when generating messages to be sent to transport address.
- `IPAddress` - Configures an IP target address to which the generated SNMP notifications are sent.
- `IP6Address` - Configures an IP6 target address to which the generated SNMP notifications are sent.
- `timeout<Seconds(1-1500)>` - Sets the time in which the SNMP agent waits for a response from the SNMP Manager before retransmitting the Inform Request Message. The value ranges between 1 and 1500 seconds.
- `retries<RetryCount(1-3)>` - Sets the maximum number of times the agent can retransmit the Inform Request Message. This value ranges between 1 and 3.
- `taglist<TagIdentifier | none>` - Sets the tag identifier that selects the target address for the SNMP. The taglist can also be set as none using the none option.
- `volatile` - Sets the storage type as temporary. Erases the configuration setting on restarting the system

- **nonvolatile** - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration can be viewed on restarting the system.
- **port <integer (1-65535)>** - Configures a port number through which the generated SNMP notifications are sent to the target address. The value ranges between 1 and 65535.

Mode Global Configuration Mode

Default

- ParamName - Internet
- IPAddress - 10.0.0.10
- taglist - snmp
- volatile | nonvolatile - volatile
- port – 162

☞ Target param must have been configured.

Example

```
Your Product (config)# snmp targetaddr smismgr param smisd 10.0.0.10 taglist mytag nonvolatile
```

Related Command(s)

- **snmp targetparams** - Configures the SNMP target parameters
- **show snmp targetaddr** - Displays the configured SNMP target Addresses
- **show snmp targetparam** - Displays the configured SNMP Target Address Params

---

10.13 snmp targetparams

Command Objective

This command configures the SNMP target parameters.

The no form of the command removes the SNMP target parameters.

Syntax

```
snmp targetparams <ParamName> user <UserName>
security- model {v1 | v2c | v3 {auth | noauth |
priv}} message- processing {v1 | v2c | v3}
[{volatile | nonvolatile}] [filterprofile-name
<profilename> ] [filter-storagetype{volatile |
nonvolatile}]

no snmp targetparams <ParamName>
```

Parameter Description

- `<ParamName>` - Sets a unique identifier of the parameter.
- `User <UserName>` - Sets a user for which the target parameter is to be done.
- `security-model` - Sets the security model
- `v1` – Sets the SNMP version as Version 1.
- `v2c` – Sets the SNMP version as Version 2.
- `v3` – Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word
- `auth` - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication
- `noauth` - Sets no-authentication
- `priv` - Specifies both authentication and privacy
- `message-processing` - Sets the message processing model
  - `v1` – Sets the SNMP version as Version 1.
  - `v2c` – Sets the SNMP version as Version 2.
  - `v3` – Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word
- `volatile` - Sets the storage type as temporary. Erases the configuration setting on restarting the system
- `nonvolatile` - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration can be viewed on restarting the system.

- **filterprofile-name <profilename>** – Configures the profile name
- **filter-storagetype**- Sets the required storage type for the filter profile
  - **volatile** – Sets the storage type as temporary. Erases the configuration setting on restarting the system.
  - **nonvolatile**– Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.

Mode

Global Configuration Mode

Default

- Target ParamName - internet
- User/Security Name - None
- Security Model - v2c
- Security Level - NoauthNoPriv
- Message Processing Model - v2c
- Storage Type - Non-volatile
- Row status - Active
- Filter profile name - None
- ParamName - test1
- User/Security Name - None
- Security Model - v1
- Security Level - NoauthNoPriv
- Message Processing Model - v1
- Storage Type - Non-volatile
- Row status - Active
- Filter profile name – None

☞ User information must have been configured prior to the configuration of SNM target parameters

---

Example

```
Your Product (config)# snmp targetparams param1
user user1 security-model v3 noauth message-
processing v3
```

Related Command(s)

- `snmp user` - Configures the SNMP user details
- `snmp targetaddr` - Configures the SNMP target address

- `show snmp targetparam` - Displays the configured SNMP Target Address Params
- `show snmp user` - Displays the configured SNMP users.
- `show snmp notif` - Displays the configured SNMP Notifications

10.14 snmp user

Command Objective

This command configures the SNMP user details.

The no form of the command removes the SNMP user details.

Syntax

```
snmp user <UserName> [auth {md5 | sha} <passwd>
[priv {{{DES | AES_CFB128} <passwd> } | None}]]
[{volatile | nonvolatile}] [EngineId <EngineID>]

no snmp user <UserName> [EngineId <EngineID>]
```

Parameter

Description

- **<UserName>** - Configures an user name which is the User-based Security Model dependent security ID.
- **auth** - Sets an authentication Algorithm . Options are:
  - **md5** - Sets the Message Digest 5 based authentication.
  - **sha** - Sets the Security Hash Algorithm based authentication.
- **<Passwd>** - Sets the authentication password that will be used for the configured authentication algorithm.
- **priv** - Sets the DES encryption and also the password to be used for the encryption key. Options are:
  - **DES** – Configures the data encryption standard algorithm related configuration.
  - **AES_CFB128** – Configures Advanced Encryption Standard (AES)
- algorithm for encryption.
  - **<Passwd>** - Sets the authentication password that will be used for the configured authentication algorithm.
  - **None -** Sets encryption configuration as none.
- **volatile** - Sets the storage type as temporary. Erases the configuration setting on restarting the system
- **nonvolatile** - Sets the storage type as permanent. Saves the configuration to the system. You can view the saved configuration on restarting the system
- **EngineId <EngineID>** - Sets the engine ID that is utilized as a unique identifier of a SNMPv3 engine. This engine ID is used to identify a source SNMPv3 entity and a destination SNMPv3 entity to

coordinate the exchange of messages between the source and the destination.

Mode Global Configuration Mode

Default

- UserName - Initial
- Authentication Protocol - None
- Privacy Protocol - None
- Storage type - Non-volatile

☞ SNMP passwords are localized using the local SNMP engine ID

Example

```
Your Product (config)# snmp user user1
```

Related Command(s)

- `show snmp engineID` - Displays the Engine Identifier
- `show snmp user` - Displays the configured SNMP users
- `snmp targetparams` - Configures the SNMP target parameters
- `show snmp group` – Displays the configured SNMP groups

10.15 snmp notify

Command Objective This command configures the SNMP notification details.

The no form of this command removes the SNMP notification details.

Syntax

```
snmp notify <NotifyName> tag <TagName> type
{Trap | Inform} [{volatile | nonvolatile}]

no snmp notify <NotifyName>
```

Parameter

Description

- `<NotifyName>` - Configures a unique identifier associated with the entry.
- `tag<TagName>` - Sets a notification tag, which selects the entries in the Target Address Table.
- `type` - Sets the notification type. The list contains:
  - `Trap` – Allows routers to send traps to SNMP managers. Trap is a one-way message from a network element such as a router, switch or server; to the network management system.
  - `Inform` – Allows routers / switches to send inform requests to SNMP managers
- `volatile` - Sets the storage type as temporary. Erases the configuration setting on restarting the system.
- `nonvolatile` - Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system

Mode Global Configuration Mode

Default

- Notify Name - smis1
- Notify Tag - smis1
- Storage type - volatile

Example

```
Your Product (config)# snmp notify note1 tag tag1
type Inform
```

Related Command(s)

- `show snmp notif` - Displays the configured SNMP Notifications
- `show snmp targetaddr` - Displays the configured SNMP target Addresses

10.16 snmp filterprofile

Command Objective

This command creates Notify filter Profile entry.

The no form of the command removes the filter entry from the table.

Syntax

```
snmp filterprofile <profile-name> <OIDTree>
[mask<OIDMask>] {included | excluded} [{volatile |
nonvolatile}]

no snmp filterprofile <profilename> <OIDTree>
```

Parameter

Description

- `profile-name` - Configures the name of the filter profile. This is a string value with a maximum size as 32.
- `OIDTree` - Configures the object Identifier
- `mask <OIDMask>` - Defines a family of subtrees, in combination with the object identifier.
- `included | excluded` - Configures the type of filter. This indicates whether the family of subtrees defined by the OID and mask should be included in or excluded from the filter profile.
- `volatile | nonvolatile` - Specifies the storage type. The list contains;
  - `volatile` - Temporary storage. Details are lost once restarted.
  - `nonvolatile` - Permanent storage. Details are present even after restart.

Mode

Global Configuration Mode

Example

```
Your Product (config)# snmp filterprofile filter1
1.5 mask 1.1 included nonvolatile
```

Related Command(s)

- `show snmp filter` - Displays the configured SNMP filters
- `snmp targetparams` - Configures the SNMP target parameters

10.17 snmp-server enable traps snmp authentication

Command Objective	This command enables generation of authentication traps from the snmp agent (for all snmpv1, snmpv2 and snmpv3) The no form of the command disables generation of authentication traps.

Syntax	`snmp-server enable traps snmp authentication`
	
	`no snmp-server enable traps snmp authentication`

Mode	Global Configuration Mode
Default	Disabled
Example	`Your Product (config)# snmp-server enable traps snmp authentication`

10.18 snmp-server trap udp-port

Command Objective	This command configures the udp port over which agent sends the trap. The no form of the command configures the snmp agent to send trap on default udp port.

Syntax	`snmp-server trap udp-port <port>`
	
	`no snmp-server trap udp-port`

Mode	Global Configuration Mode
Example	`Your Product (config)# snmp-server trap udp-port 1234`
Related Command(s)	• `show snmp notif` - Displays the configured SNMP Notification types.

10.19 snmp-server trap proxy-udp-port

Command Objective	This command configures the udp port over which agent sends the trap to the proxy entity. The no form of the command configures the snmp agent to send trap on default udp port.

Syntax	`snmp-server trap proxy-udp-port <port>`
	
	`no snmp-server trap proxy-udp-port`

Mode	Global Configuration Mode
Default	162
Example	`Your Product (config)# snmp-server trap proxy-udp-port 162`
Related Command(s)	• `show snmp-server proxy-udp-port` - Displays the proxy udp port.

10.20 snmp agent port

Command Objective	This command configures the agent port on which agent listens. The port number value ranges between 1 and 65535.
Syntax	`snmp agent port <port>`
Mode	Global Configuration Mode
Default	161
Example	`Your Product (config)# snmp agent port 100`

Related Command(s)

- `show snmp` - Displays the status information of SNMP communications

10.21 snmp tcp enable

Command Objective	This command enables sending snmp messages over tcp. The no form of the command disables sending snmp messages over tcp.

Syntax	`snmp tcp enable`
	
	`no snmp tcp enable`

Mode	Global Configuration Mode
Default	Disabled
Example	`Your Product (config)# snmp tcp enable`
Related Command(s)	• `show snmp tcp` - Displays the configuration for snmp over tcp.

10.22 snmp trap tcp enable

Command Objective

This command enables sending snmp trap messages over tcp.

The no form of the command disables sending snmp trap messages over tcp.

Syntax

```
snmp trap tcp enable

no snmp trap tcp enable
```

Mode

Global Configuration Mode

Default

Disabled

Example

```
Your Product (config)# snmp trap tcp enable
```

Related Command(s)

- `show snmp tcp` - Displays the configuration for snmp over tcp.

10.23 snmp-server tcp-port

Command Objective	This command configures the tcp port over which agent sends the snmp message. This value ranges between 1 and 65535. The no form of the command configures the snmp agent to send snmp message on default tcp port.

Syntax	`snmp-server tcp-port <port>`
	
	`no snmp-server tcp-port`

Mode	Global Configuration Mode
Default	161
Example	`Your Product (config)# snmp-server tcp-port 161`
Related Command(s)	• `show snmp tcp` - Displays the configuration for snmp over tcp.

10.24 snmp-server trap tcp-port

Command Objective	This command configures the tcp port over which agent sends the trap. This value ranges between 1 and 65535. The no form of the command configures the snmp agent to send trap on default tcp port.

Syntax	`snmp-server trap tcp-port <port>`
	
	`no snmp-server trap tcp-port`

Mode	Global Configuration Mode
Default	162
Example	`Your Product (config)# snmp-server trap tcp-port 162`
Related Command(s)	• `show snmp tcp` - Displays the configuration for snmp over tcp.

10.25 snmp-server enable traps

Command Objective	This command enables generation of a particular trap. The no form of the command disables generation of a particular trap.

Syntax	`snmp-server enable traps {[firewall-limit] [linkup] [linkdown] [sip-states] [sip-cfg-change] [coldstart] [poe- power] [dhcp-pool-limit] [dsx1-line]}`
	
	`no snmp-server enable traps {[firewall-limit] [linkup] [linkdown] [sip-states] [sip-cfg-change] [coldstart] [poe- power] [dhcp-pool-limit] [dsx1-line]}`

Parameter Description	• `firewall-limit` - Generates a trap for all the firewall attack summary • `linkup` - Generates a trap whenever there is a linkup • `linkdown` - Generates a trap whenever there is a linkdown • `sip-states` - Generates a trap for all the SIP states. • `sip-cfg-change` - Generates a trap for all the SIP configuration • `coldstart` - Generates a trap for all the Coldstart • `poe-power` - Generates a trap whenever there is Power on Ethernet • `dhcp-pool-limit` - Generates a trap for all the DHCP server pool limit trap • `dsx1-line` - Generates a trap for all the DSX1 line trap
Mode	Global Configuration Mode
Example	`Your Product (config)# snmp-server enable traps firewall- limit`
Related Command(s)	• `show snmp-server traps` - Displays the set of traps that are currently enabled.

10.26 show snmp agentx information

Command Objective	This command displays global information of SNMP Agentx communications.
Syntax	`show snmp agentx information`
Mode	Privileged EXEC Mode

Example	`Your Product# show snmp agentx information`
	`Agentx Subagent is enabled`
	`TransportDomain: TCP Master`
	`IP Address: 10.0.0.2`
	`Master PortNo: 705`

Related Command(s)	• `enable snmpsubagent` - Enables agentx-subagent capabilities. • `disable snmpsubagent` – Disables agentx-subagent. • `disable snmpagent` - Disables SNMP agent.

10.27 show snmp agentx statistics

Command Objective	This command displays all the information regarding SNMP Agentx statistics.
Syntax	`show snmp agentx statistics`
Mode	Privileged EXEC Mode

Example	**`Your Product# show snmp agentx statistics`**
	`Tx Statistics`
	`Transmitted Packets: 860`
	`Open PDU: 1`
	`Index Allocate PDU: 0`
	`Index DeAllocate PDU: 0`
	`Register PDU: 2`
	`Add Agent Capabilities PDU: 0`
	`Notify PDU: 0`
	`Ping PDU: 20`
	`Remove Agent Capabilities  PDU: 0`
	`Close PDU: 0`
	`Response PDU: 0`
	`Rx: 83`
	`Statistics: 7`
	`Rx Packets: 1`
	`Get PDU: 83`
	`GetNext PDU: 6`

```
GetBulk PDU: 0

TestSet PDU: 0

Commit PDU: 0

Cleanup PDU: 0

Undo PDU: 0

Dropped Packets: 0

Parse Drop Errors: 1

Open Fail Errors: 0

Close PDU Response PDU: 0
```

Related Command(s)

- **enable snmpsubagent** - Enables agentx-subagent capabilities.
- **disable snmpsubagent** – Disables agentx-subagent.
- **disable snmpagent** - Disables snmp agent

10.28 show snmp

Command Objective	This command displays the status information of SNMP communications.
Syntax	`show snmp`
Mode	Privileged EXEC Mode

Example	`Your Product# show snmp`
	`0 SNMP Packets Input`
	`0 Bad SNMP Version errors`
	`0 Unknown community name`
	`0 Get request PDUs`
	`0 Get Next PDUs`
	`0 Set request PDUs`
	`0 SNMP Packets Output`
	`0 Too big errors`
	`0 No such name errors`
	`0 Bad value errors`
	`0 General errors`
	`0 Trap PDUs`
	`0 SNMP Rollback failures`
	`SNMP Manager-role output packets`
	`0 Drops`
	`SNMP Informs:`
	`0 Inform Requests generated`

```
0 Inform Responses received

0 Inform messages Dropped

0 Inform Requests awaiting Acknowledgement

SNMP Trap Listen Port is 162 snmp agent port : 170
```

Related Command(s)

- **snmp community index** - Configures the SNMP community details

---

10.29 show snmp community

Command Objective	This command displays the configured SNMP community details.
Syntax	`show snmp community`
Mode	Privileged EXEC Mode

Example

```
Your Product# show snmp community

Community Index: NETMAN Community
Name: NETMAN Security Name: none
Context Name:

Transport Tag:

Storage Type: volatile

Row Status: active

------------------------------
Community Index: PUBLIC Community
Name: PUBLIC

Security Name: none
Context Name: Transport
Tag:

Storage Type: volatile

Row Status: active
```

Related Command(s)

- `snmp community index` - Configures the SNMP community details

10.30 show snmp group

Command Objective	This command displays the configured SNMP groups.
Syntax	`show snmp group`
Mode	Privileged EXEC Mode
Example	`Your Product# show snmp group` Security Model: v1 Security Name: none Group Name: iso Storage Type: volatile Row Status: active --------------------------- Security Model: v2c Security Name: none Group Name: iso Storage Type: volatile Row Status: active --------------------------- Security Model: v3 Security Name: initial Group Name: initial Storage Type: nonVolatile Row Status: active --------------------------- Security Model: v3

```
Security Name: templateMD5
Group Name: initial
Storage Type: nonVolatile
Row Status: active

Security Model: v3
Security Name: templateSHA
Group Name: initial
Storage Type: nonVolatile
Row Status: active
```

Related Command(s)

- **snmp group** - Configures the SNMP group details
- **snmp access** - Configures the SNMP group access details
- **snmp user** - Configures the SNMP user details
- **snmp proxy name** – Configures the proxy.
- **snmp mibproxy name** – Configures the mibproxy.

10.31 show snmp group access

Command Objective	This command displays the configured SNMP group access details.
Syntax	`show snmp group access`
Mode	Privileged EXEC Mode

Example

```
Your Product# show snmp group access

Group Name: iso
Read View: iso
Write View: iso
Notify View: iso

Storage Type: volatile

Row Status: active

---------------------------

Group Name: iso

Read View: iso
Write View: iso
Notify View: iso

Storage Type: volatile

Row Status: active

---------------------------

Group Name: initial

Read View: restricted

Write View: restricted
Notify View: restricted
```

```
Storage Type: nonVolatile
Row Status: active

------------------------------

Group Name: initial

Read View: iso
Write View: iso
Notify View: iso

Storage Type: nonVolatile

Row Status: active
```

Related Command(s)

- **snmp access** - Configures the SNMP group access details
- **snmp view** - Configures the SNMP view

10.32 show snmp engineID

Command Objective	This command displays the Engine Identifier.
Syntax	`show snmp engineID`
Mode	Privileged EXEC Mode
Example	`Your Product# show snmp engineID` `EngineId: 80.00.08.1c.04.46.53`
Related Command(s)	• `snmp engineid` - Configures the engine identifier • `snmp user` - Configures the SNMP user details

10.33 show snmp proxy

Command Objective	This command displays proxy details.
Syntax	`show snmp proxy`
Mode	Privileged EXEC Mode

Example

```
Your Product# show snmp proxy
Proxy Name: PROXY1
Proxy ContextEngineID: 80.00.08.1c.04.46.54
Proxy ContextName:
Proxy TargetParamIn: param1
Proxy SingleTargetOut: Tgt1
Proxy MultipleTargetOut:
Proxy Type: Read
Storage Type: Non-volatile
Row Status: Active
-----------------------------------------------
Proxy Name: PROXY2
Proxy ContextEngineID: 80.00.08.1c.04.46.54
Proxy ContextName:
Proxy TargetParamIn: param1
Proxy SingleTargetOut: Tgt1
Proxy MultipleTargetOut:
Proxy Type: Write
Storage Type: Non-volatile
```

```
Row Status: Active

---------------------------------------------------
```

Related Command(s)

- **snmp proxy name** - Configures the proxy.

10.34 show snmp mibproxy

Command Objective	This command displays proxy details.
Syntax	`show snmp mibproxy`
Mode	Privileged EXEC Mode

Example	**`Your Product# show snmp mibproxy`**
	`Prop Proxy Name: proxy1`
	`Prop MibID: 2`
	`Prop Proxy TargetParamIn: param1`
	`Prop Proxy SingleTargetOut: target1`
	`Prop Proxy MultipleTargetOut:`
	`Prop Proxy Type: Read`
	`Prop Storage Type: Non-volatile`
	`Prop Row Status: Active`
	`----------`

Related Command(s)	• **`snmp mibproxy name`** - Configures the proxy.

10.35 show snmp viewtree

Command Objective	This command displays the configured SNMP Tree views.
Syntax	`show snmp viewtree`
Mode	Privileged EXEC Mode

Example

```
Your Product# show snmp viewtree

View Name: iso

Subtree OID: 1

Subtree Mask:

View Type: included Storage

Type: nonVolatile Row Status: active

----------------------------
View Name: restricted

Subtree OID: 1

Subtree Mask:

View Type: included
Storage Type: nonVolatile
Row Status: active

------------------------------
```

Related Command(s)

- `snmp access` - Configures the SNMP group access details
- `snmp view` - Configures the SNMP view

10.36 show snmp targetaddr

Command Objective	This command displays the configured SNMP target Addresses.
Syntax	`show snmp targetaddr`
Mode	Privileged EXEC Mode

Example	`Your Product# show snmp targetaddr`
	`Target Address Name: ht231`
	`IP Address: 12.0.0.100`
	`Port: 150`
	`Tag List: tg231`
	`Parameters: pa231`
	`Storage Type: Non-volatile`
	`Row Status: Active`
	`------------------------------`

Related Command(s)

- `snmp targetaddr` - Configures the SNMP target address
- `snmp targetparams` - Configures the SNMP target parameters
- `snmp notify` - Configures the SNMP notification details

10.37 show snmp targetparam

Command Objective	This command displays the configured SNMP Target Address Params.
Syntax	`show snmp targetparam`
Mode	Privileged EXEC Mode

Example	**`Your Product# show snmp targetparam`**
	`Target Parameter Name: internet Message`
	`Processing Model: v2c`
	`Security Model: v2c`
	`Security Name: none`
	`Security Level: No Authentication, No Privacy`
	`Storage Type: Non-volatile`
	`Row Status: Active Filter`
	`Profile Name: None`
	`Row Status: Active`
	`----------------------------`
	`Target Parameter Name: pa231`
	`Message Processing Model: v3`
	`Security Model: v3`
	`Security Name: u231`
	`Security Level: No Authentication, No Privacy`

```
Storage Type: Volatile Row
Status: Active Filter Profile
Name: filter1

Row Status: Active

-----------------------------
Target Parameter Name: test1

Message Processing Model: v2c
Security Model: v1
Security Name: none
Security Level: No Authentication, No Privacy
Storage Type: Non-volatile
Row Status: Active
Filter Profile Name: None
Row Status: Active
------------------------------
```

Related Command(s)

- **snmp targetaddr** - Configures the SNMP target address
- **snmp targetparams** - Configures the SNMP target parameters
- **snmp user** - Configures the SNMP user details

10.38 show snmp user

Command Objective	This command displays the configured SNMP users.
Syntax	`show snmp user`
Mode	Privileged EXEC Mode

Example	**`Your Product# show snmp user`**
	`Engine ID: 80.00.08.1c.04.46.53`
	`User: initial`
	`Authentication Protocol: none`
	`Privacy Protocol: none`
	`Storage Type: nonvolatile`
	`Row Status: active`
	`----------------------------`
	`Engine ID: 80.00.08.1c.04.46.53`
	`User: templateMD5`
	`Authentication Protocol: MD5`
	`Privacy Protocol: none`
	`Storage Type: nonVolatile Row`
	`Status: active`
	`----------------------------`
	`Engine ID: 80.00.08.1c.04.46.53`
	`User: templateSHA`
	`Authentication Protocol: SHA`

```
Privacy Protocol: DES_CBC

Storage Type: nonVolatile

Row Status: active

------------------------------
```

Related Command(s)

- **snmp group** - Configures the SNMP group details
- **snmp user** - Configures the SNMP user details
- **show snmp community** - Displays the configured SNMP community details
- **snmp engineid** - Configures the engine identifier
- **snmp targetparams** - Configures the SNMP target parameters

---

10.39 show snmp notif

Command Objective	This command displays the configured SNMP Notification types.
Syntax	`show snmp notif`
Mode	Privileged EXEC Mode

Example	`Your Product# show snmp notif`
	`Notify Name: smis`
	`Notify Tag: smis`
	`Notify Type: trap`
	`Storage Type: volatile`
	`Row Status: active`
	`---------------------------`
	`Notify Name: smis1`
	`Notify Tag: smis1`
	`Notify Type: trap`
	`Storage Type: volatile`
	`Row Status: active`

Related Command(s)

- `snmp notify` - Configures the SNMP notification details
- `snmp targetparams` - Configures the SNMP target parameters
- `snmp-server trap udp-port`- Configures the udp port over which agent sends the trap

10.40 show snmp inform statistics

Command Objective	This command displays the inform message statistics.
Syntax	`show snmp inform statistics`
Mode	Privileged EXEC Mode
☞	SNMP Manager must have been configured and Inform type notifications must have been generated.

Example	**`Your Product# show snmp inform statistics`**
	`Target Address Name: smismanager`
	`IP Address: 10.0.0.10`
	`Inform messages sent: 20`
	`Acknowledgement awaited for: 2 Inform messages`
	`Inform messages dropped: 0`
	`Acknowledgement failed for: 0 Inform messages`
	`Informs retransmitted: 0`
	`Inform responses received: 18`

10.41 show snmp-server traps

Command Objective	This command displays the set of traps that are currently enabled.
Syntax	`show snmp-server traps`
Mode	Privileged EXEC Mode
Example	`Your Product# show snmp-server traps` `Currently enabled traps: linkup,linkdown,`
Related Command(s)	• `snmp-server enable traps` - Enables generation of a particular trap.

10.42 show snmp-server proxy-udp-port

Command Objective This command displays the proxy udp port.

Syntax

```
show snmp-server proxy-udp-port
```

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp-server proxy-udp-port
snmp-server proxy-udp-port : 162
```

Related Command(s)

- `snmp-server trap proxy-udp-port` - Configures the udp port over which agent sends the trap.

10.43 show snmp tcp

Command Objective	This command displays the configuration for snmp over tcp.
Syntax	`show snmp tcp`
Mode	Privileged EXEC Mode

Example	`Your Product# show snmp tcp`
	`snmp over tcp disabled`
	`snmp trap over tcp disabled`
	`snmp listen tcp port 161`
	`Snmp listen tcp trap port 162`

Related Command(s)	• `snmp tcp enable` – Enables sending snmp messages over tcp. • `snmp trap tcp enable` - Enables sending snmp trap messages over tcp. • `snmp-server tcp-ports` – Configures the tcp port over which agent sends the snmp message. • `snmp-server trap tcp-ports` - Configures the tcp port over which agent sends the trap.

10.44 show snmp filter

Command Objective This command displays the configured SNMP filters.

Syntax

```
show snmp filter
```

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp filter

Filter Name: filter1

Subtree OID: 1.5

Subtree Mask: 1.1

Filter Type: Included

Storage Type: Non-volatile

Row Status: Active

------------------------------
```

Related Command(s)

- `snmp filterprofile` - Creates Notify filter Table

10.45 snmpset mib

Command Objective	This command sets the value of the mib object through SNMP agent.

This command is intended for internal testing purpose only

Syntax

```
snmpset mib {name | oid} <name/oid> value <string>
  [short] [<datatype - i, o, x, s>]
```

Parameter

Description

- `name <name> -` Sets the mib object name. This is a string value with maximum size as 32.
- `oid <oid> -` Sets the mib object identifier. This is a string value with maximum size as 32.
- `value <string> -` Sets the value for the mib object.
- `short -` Displays the value of the mib object.
- `datatype -` Sets the specified datatype for the mib object. The data types are

  – i – Sets the integer value for the mib object.

  – s - Sets the string value for the mib object.

  – o - Sets the Octet string value for the mib object.

  – x - Sets the hexa string value for the mib object.

Mode Global Configuration Mode

Example

```
Your Product (config)# snmpset mib name
snmpListenTcpPort.0 value 145 short 1
```

Related Command(s)

- `show snmp` - Displays the status information of SNMP communications.
- `show mib name` – Displays the name of the corresponding Object Identifier.
- `show mib oid` - Displays the OID (Object Identifier) of the corresponding mib object.

10.46 snmpget mib

Command Objective	This command gets the value of the mib object through SNMP agent.
	This command is intended for internal testing purpose only
Syntax	`snmpget mib {name | oid} <value> [short]`
Parameter **Description**	• `name <value> -` Gets the mib object name. This is a string value with maximum size as 32. • `oid <value> -` Gets the mib object identifier. This is a string value with maximum size as 32. • `short -` Displays the value of the mib object.
Mode	Global Configuration Mode
Example	`Your Product (config)# snmpget mib name fsbgp4PeerExtConfigurePeer.12.0.0.1 short`
Related Command(s)	• `show snmp` - Displays the status information of SNMP communications. • `snmpset mib` - Sets the value of the mib object via SNMP agent.

10.47 snmpgetnext mib

Command Objective	This command gets the next mib object for the given object.
	This command is intended for internal testing purposes only
Syntax	`snmpgetnext mib {name | oid} <value> [short]`
Parameter **Description**	• `name <value> -` Gets the next mib object name. This is a string value with maximum size as 32. • `oid <value> -` Gets the next mib object identifier. This is a string value with maximum size as 32. • `short -` Displays the value of the mib object.
Mode	Global Configuration Mode
Example	`Your Product (config)# snmpgetnext mib name fsbgp4PeerExtTable short`
Related Command(s)	• `show snmp` - Displays the status information of SNMP communications.

10.48 snmpwalk mib

Command Objective	This command displays all the mib objects of the given table.
	This command is intended for internal testing purpose only
Syntax	`snmpwalk mib {name | oid} <value> [count <integer(1-100)>] [short]`
Parameter **Description**	• `name <value>` - Gets the next mib object name for the given mib object name. This is a string value with maximum size as 32. • `oid <value>` - Gets the next mib object identifier for the given mib object identifier. • `count <integer(1-100)>` - Sets the number of entries to be displayed in the mib object. This value ranges between 1 and 100. • `short` - Displays the value of the mib object.
Mode	Global Configuration Mode
Example	`Your Product (config)# snmpwalk mib name fsbgp4PeerExtTable`

10.49 snmp filter trap

Command Objective	This command sets the traps to be filtered. The no form of the command removes the traps from filter table.

Syntax	`snmp filter trap {name | oid} <name/oid>`
	
	`no snmp filter trap {name | oid} <name/oid>`

Parameter **Description**	• `name <name>` - Gets the mib object name. This is a string value with maximum size as 32. • `oid <oid>` - Gets the mib object identifier.
Mode	Global Configuration Mode
Example	`Your Product (config)# snmp filter trap name fsbgp4PeerExtTable`

10.50 show mib oid

Command Objective This command displays the OID (Object Identifier) of the corresponding mib object name.

This command is intended for internal testing purpose only

Syntax `show mib oid <object name. eg ifMainRowStatus>`

Mode Privileged EXEC Mode

Example

```
Your Product (config)#  show mib oid
fsbgp4PeerExtTable

MIB OID for fsbgp4PeerExtTable is
1.3.6.1.4.1.2076.41.2
```

Related Command(s)

- `snmpset mib` - Sets the value of the mib object via SNMP agent.

10.51 show mib name

Command Objective	This command displays the name of the corresponding mib object identifier.
	This command is intended for internal testing purposes only
Syntax	`show mib name <Object OID. eg 1.3.6.1.6>`
Mode	Privileged EXEC Mode
Example	**`Your Product (config)# show mib name 1.3.6.1.4.1.2076.41.2`** `MIB Name for 1.3.6.1.4.1.2076.41.2 is fsbgp4PeerExtTable`
Related Command(s)	• `snmpset mib` - Sets the value of the mib object via SNMP agent.

11 Syslog

Syslog is a protocol used for capturing log information for devices on a network. The syslog protocol provides a transport to allow a machine to send event notification messages across IP networks to event message collectors, also known as syslog servers. The protocol is simply designed to transport the event messages.

One of the fundamental tenets of the syslog protocol and process is its simplicity. The transmission of syslog messages may be started on a device without a receiver being configured, or even actually physically present. This simplicity has greatly aided the acceptance and deployment of syslog.

The list of CLI commands for the configuration of syslog is as follows:

- `Logging`
- `logging synchronous`
- `mailserver`
- `sender mail-id`
- `cmdbuffs`
- `clear logs`
- `syslog mail`
- `syslog local storage`
- `syslog filename-one`
- `syslog filename-two`
- `syslog filename-three`
- `syslog relay - port`
- `syslog profile`
- `logging-file`
- `logging server`
- `syslog relay`
- `syslog relay transport type`
- `show logging`
- `show email alerts`
- `show syslog role`
- `show syslog mail`
- `show syslog localstorage`
- `show logging-file`
- `show logging-server`
- `show mail-server`
- `show syslog relay-port`
- `show syslog profile`
- `show syslog relay transport type`
- `show syslog file-name`

- show syslog information
- smtp authentication
- snmp trap syslog-server-status

11.1 Logging

Command Objective

This command enables syslog server and configures the syslog related parameters. The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or syslog server.

The no form of the command disables syslog server and resets the configured parameters. The existing syslog buffers will not be cleared and none of the configured options will be changed, when the syslog feature is disabled.

Syntax

```
logging { buffered [<size (1-200)>] | console |
facility

{local0 | local1 | local2 | local3 | local4 | local5 |

local6 | local7|}| severity [{ <level (0-7)> |
alerts |

critical | debugging | emergencies | errors |
informational

| notification | warnings }] | on }

no logging { buffered | console | facility |
severity | on}
```

Parameter

Description

- `buffered` - Limits Syslog messages displayed from an internal buffer. This size ranges between 1 and 200 entries.

  The size feature is optional only in the code using standard command, otherwise this feature is mandatory.

- `console` - Limits messages logged to the console.
- `facility` - The facility that is indicated in the message. Can be one of the following values: local0, local1, local2, local3, local4, local5, local 6, local7.
- `severity` - Message severity level. Messages with severity level equal to or high than the specified value are printed asynchronously. This can be configured using numerical value or using the available option. The options are:
  - `0 | emergencies` - System is unusable.

- 1 | alerts - Immediate action needed.
- 2 | critical - Critical conditions.
- 3 | errors - Error conditions.
- 4 | warnings - Warning conditions.
- 5 | notification - Normal but significant conditions.
- 6 | informational - Informational messages.
- 7 | debugging – Debugging messages.

- alerts - Immediate action needed
- critical - Critical conditions
- debugging - Debugging messages
- emergencies - System is unusable
- errors - Error conditions
- informational - Information messages
- notification - Normal but significant messages
- warnings - Warning conditions
- on - Syslog enabled

Mode Global Configuration Mode

Default

- console - enabled
- severity - informational, when no option is selected while configuration.
- debugging, at system start-up.
- buffered - 50
- facility - local0

☞ The log file is stored in ASCII text format. The Privileged EXEC command is used to display its contents

- The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or Syslog server
- The existing syslog buffers will not be cleared and none of the configured options will be changed, when the Syslog feature is disabled

---

Example

```
Your Product (config)# logging buffered
```

Related Command(s)	• `show logging` - Displays Logging status and configuration information

11.2 logging synchronous

Command Objective

This command enables synchronous logging of messages.

This command is a complete standardized implementation of the existing command. It operates similar to that of the command logging.

Syntax

```
logging synchronous {severity [{<short (0-7)> |
alerts | critical | debugging | emergencies |
errors | informational | notification |
warnings|all}] | limit

<number-of-buffers(size(1-200))}
```

Parameter

Description

- `severity` - Message severity level. Messages with severity level equal to or high than the specified value are printed asynchronously. This can be configured using numerical value or using the available option. The options are:
- `0 | emergencies` - System is unusable.
- `1 | alerts` - Immediate action needed.
- `2 | critical` - Critical conditions.
- `3 | errors` - Error conditions.
- `4 | warnings` - Warning conditions.
- `5 | notification` - Normal but significant conditions.
- `6 | informational` - Informational messages.
- `7 | debugging` – Debugging messages.
- `all` - All messages are printed asynchronously regardless of the severity level.

- `limit <number-of-buffers(size(1-200)` - Number of buffers to be queued for the terminal after which new messages are dropped. This value ranges between 1 and 200 entries.

Mode

Line Configuration Mode

Default

- severity - informational, when no option is selected while configuration. debugging, at system start-up.
- limit - 50

The log file is stored in ASCII text format. The Privileged EXEC command is used to display its contents.

- The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or Syslog server.
- The existing syslog buffers will not be cleared and none of the configured options will be changed, when the Syslog feature is disabled.

Example

```
Your Product (config-line)# logging synchronous
severity 4
```

Related Command(s)

- `show logging` - Displays Logging status and configuration information

---

11.3 mailserver

Command Objective	This command sets the mail server IP address to be used for sending email alert messages. The no form of the command re-sets the mail server IP address used for sending email alert messages.

Syntax	`mail-server <short (0-191)> {ipv4 <ucast_addr> | ipv6 <ip6_addr> | <host-name>} <string(50)> [user <user_name> password <password>]`
	
	`no mail-server <short (0-191)> {ipv4 <ucast_addr> | ipv6 <ip6_addr> | <host-name>}`

Parameter	
Description	• `<short (0-191)>` - Sets the priority for that particular mail-server configuration. The value ranges between 0 and 191. • `ipv4<ucast_addr>` - Configures the ipv4 destination address for the syslog mail server • `ipv6<ip6_addr>` - Configures the ipv6 destination address for the syslog mail server. • `<host-name>` - Configures the host name for the syslog mail server. • `<string(50)>` - Specifies the receiver mail id in which the email alert messages are received and logged. • `user <user_name>` - Configures the user name of the account in the mail server to which the mails is to be sent. The user name is used only if a valid authentication method is configured for the system. The maximum allowed size in 64 characters. • `password <password>` - Sets the password to authenticate the user name in the mail server. The password is used only if a valid authentication method is configured for the system. The maximum allowed size in 64 characters.
Mode	Global Configuration Mode

Example

```
Your Product (config)# mail-server 190 ipv4
23.78.67.89 support@Aricent.com
```

Related Command(s)

- `logging` - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter
- `show email alerts` - Displays email alerts related configuration

11.4 sender mail-id

Command Objective	This command sets the sender mail id from which the email alert messages are sent. The no form of the command deletes the configured sender mail id.

Syntax	`sender mail-id <mail-id (100)>`
	
	`no sender mail-id`

Mode	Global Configuration Mode
Default	syslog@supermicro.com
☞	This command can be executed only if the mail server is configured.
Example	`Your Product (config)# sender mail-id plabinik@supermicro.com`

Related Command(s)

- `mailserver` - Sets the mail server IP address to be used for sending email alert messages
- `logging` - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter
- `show logging` - Displays Logging status and configuration information
- `show email alerts` - Displays email alerts related configuration
- `receiever mail-id` - Sets the receiver mail id

11.5 cmdbuffs

Command Objective	This command configures the number of syslog buffers for a particular user. This command is not supported on some SMIS models.
Syntax	`cmdbuffs <user name> <no.of buffers (1-200)>`
Parameter Description	• `<user name>`- User Name • `<no.of buffers (1-200)>`- Number of log buffers to be allocated in the system
Mode	Global Configuration Mode
Default	50
Example	`Your Product(config)#cmdbuffs Aricent 50`
Related Command(s)	• `logging` - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter • `show logging` - Displays Logging status and configuration information • `clear logs` - Clears the logs buffered in the system. • `username` - Creates a user and sets the enable password for that user with the privilege level.

11.6 clear logs

Command Objective	This command clears the system syslog buffers.
Syntax	`clear logs`
Mode	Global Configuration Mode
Example	`Your Product (config)# clear logs`

Related Command(s)

- `cmdbuffs` - Configures the number of Syslog buffers for a particular user
- `logging` - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter
- `show logging` - Displays Logging status and configuration information

11.7 syslog mail

Command Objective	This command enables the syslog mail storage in the system. By enabling syslog mail storage, SMIS sends the syslog messages as mail messages to themail-server configured in the system. The no form of command disables the mail option in syslog.

Syntax	`syslog mail`
	
	`no syslog mail`

Mode	Global Configuration Mode
Example	`Your Product (config)# syslog mail`
Related Command(s)	• `show syslog mail` - Displays the mail option in syslog. • `mail server table` - Adds an entry to mail-server table. • `show syslog information` - Displays the status of consolidated syslog log information.

11.8 syslog local storage

Command Objective	This command enables the syslog file storage to log the status in the local storage path. The no form of command disables the syslog local storage.

Syntax	`syslog localstorage`
	
	`no syslog localstorage`

Mode	Global Configuration Mode
Example	`Your Product (config)# syslog localstorage`

Related Command(s)

- `show syslog local storage` - Displays the syslog local storage.
- `syslog filename-one` - Configures the file name to store the syslog messages.
- `syslog filename-two` - Configures the file name to store the syslog messages.
- `syslog filename-three` - Configures the file name to store the syslog messages
- `logging-file` - Adds an entry in to file table
- `show syslog file-name` - Displays all the syslog local storage file names.
- `show syslog information` - Displays the status of consolidated syslog log information.

11.9 syslog filename-one

Command Objective	This command configures a first file to store the syslog messages locally. The maximum size of the file name is 32.
Syntax	`syslog filename-one <string(32)>`
Mode	Global Configuration Mode
☞	This command is executed only if syslog local storage is enabled.
Example	`Your Product (config)# syslog filename-one smis1`

Related Command(s)

- `syslog local storage` - Enables the syslog local storage
- `logging-file` - Adds an entry in to file table
- `show syslog local storage` - Displays the syslog local storage.
- `show logging-file` - Displays the Syslog file table
- `show syslog file-name` - Displays all the syslog local storage file names.

11.10 syslog filename-two

Command Objective	This command configures a second file name to store the syslog messages locally. The maximum size of the file name is 32.
Syntax	`syslog filename-two <string(32)>`
Mode	Global Configuration Mode
☞	This command is executed only if syslog local storage is enabled.
Example	`Your Product (config)# syslog filename-two smis2`

Related Command(s)

- `Syslog local storage` - Enables the syslog local storage
- `show syslog file-name` - Displays the Syslog local storage file name
- `logging-file` - Adds an entry in to file table
- `show syslog local storage` - Displays the syslog local storage.
- `show logging-file` - Displays the Syslog file table

11.11 syslog filename-three

Command Objective	This command configures a third file name to store the syslog messages locally. The maximum size of the file name is 32.
Syntax	`syslog filename-three <string(32)>`
Mode	Global Configuration Mode
☞	This command is executed only if syslog local storage is enabled.
Example	`Your Product (config)# syslog filename-three smis3`

Related Command(s)

- `syslog local storage` - Enables the syslog local storage
- `show syslog file-name` - Displays the Syslog local storage file name
- `logging-file` - Adds an entry in to file table
- `show syslog local storage` - Displays the syslog local storage.
- `show logging-file` - Displays the Syslog file table

11.12 syslog relay - port

Command Objective	This command sets the syslog port through which the relay receives the syslog messages irrespective of the transport type. The port number ranges between 0 and 65535. The no form of command sets the syslog port to default port.

Syntax	`syslog relay-port <integer(0-65535)>`
	
	`no syslog relay-port`

Mode	Global Configuration Mode
Default	514
☞	This command is executed only if syslog relay is enabled.
Example	`Your Product (config)# syslog relay-port 500`

Related Command(s)

- `syslog relay` – Changes the syslog role from device to relay
- `syslog relay transport type` - Sets the syslog relay transport type either as udp or tcp
- `show syslog relay - port` – Displays the syslog relay port
- `show syslog relay transport type` – Displays the Syslog relay transport type

11.13 syslog profile

Command Objective	This command sets the profile for reliable syslog. The no form of command sets the profile to default (raw) for Reliable Syslog.

Syntax	`syslog profile {raw | cooked}`
	
	`no syslog profile`

Parameter **Description**	• `raw` - Sets the syslog profile as raw which is the profile for the transport type beep. • `cooked` - Sets the syslog profile as cooked.
☞	This feature is not supported. It may be implemented in the future.
Mode	Global Configuration Mode
Default	Raw
Example	`Your Product (config)# syslog profile raw`
Related Command(s)	• `show syslog profile` - Displays the Syslog profile.

11.14 logging-file

Command Objective	This command adds an entry in the file table. The no form of command deletes an entry from the file table.

Syntax	`logging-file <short(0-191)> <string(32)>`
	
	`no logging-file <short(0-191)> <string(32)>`

Parameter Description	• `<short(0-191)>` - Sets the priority of syslog messages. 0-lowest priority, 191-highest priority • `<string(32)>` - Represents the file-name in which a log is done.
Mode	Global Configuration Mode
☞	This command is executed only if local storage syslog is enabled.
Example	`Your Product (config)# logging-file 134 smis1`
Related Command(s)	• `show logging-file` - Displays the Syslog file table • `syslog local storage` - Enables the syslog local storage • `syslog file-one` - Configures the first file to store the syslog messages locally. • `syslog filename-two` - Configures the second file name to store the syslog messages locally.

11.15 logging server

Command Objective

This command configures a server table to log an entry in it. The no form of command deletes an entry from the server table.

Syntax

```
logging-server <short(0-191)> {ipv4 <ucast_addr> |
ipv6

<ip6_addr> | <host-name>} [ port <integer(0-65535)>]
[{udp

| tcp | beep}]

no logging-server <short(0-191)> {ipv4 <ucast_addr>
|ipv6

<ip6_addr> | <host-name>}
```

Parameter

Description

- `<short(0-191)>` - Sets the priority for the syslog messages. 0-lowest priority, 191-highest priority.
- `ipv4 <ucast_addr>` - Sets the server address type as internet protocol version 4.
- `ipv6 <ip6_addr>` - Sets the server address type as internet protocol version 6.
- `<host-name>` - Configures the host name for a server to log an entry.
- `port<integer(0-65535)>` - Sets the port number through which it sends the syslog message. The value ranges between 0 and 65535.
- `udp` - Sets the forward transport type as udp.,
- `tcp` - Sets the forward transport type as tcp,
- `beep` - Sets the forward transport type as beep.

Mode

Global Configuration Mode

Example

```
Your Product (config)# logging-server 134 ipv4
12.0.0.3
```

Related Command(s)

- `show logging-server` - Displays the Syslog logging server table

11.16 syslog relay

Command Objective	This command changes the syslog role from device to relay. The no form of command changes the syslog role from relay to device.

Syntax	`syslog relay`
	
	`no syslog relay`

Mode	Global Configuration Mode
Example	`Your Product (config)# syslog relay`

Related Command(s)

- `show syslog relay-port` - Displays the syslog relay port
- `show syslog role` – Displays the syslog role.
- `syslog relay transport type` – Sets the syslog relay transport type either as udp or tcp
- `syslog relay - port -` Sets the syslog port through which it receives the syslog messages
- `show syslog relay transport type` – Displays the Syslog relay transport type
- `show syslog information` - Displays the status of consolidated syslog log information.

11.17 syslog relay transport type

Command Objective	This command sets the Syslog relay transport type either as udp or tcp.
Syntax	`syslog relay transport type {udp | tcp}`
Parameter Description	• `udp` - Sets the relay transport type as udp • `tcp` - Sets the relay transport type as tcp
Mode	Global Configuration Mode
☞	This command is executed only if syslog relay is enabled.
Example	`Your Product (config)# syslog relay transport type udp`
Related Command(s)	• `syslog relay` – Changes the syslog role from device to relay • `show syslog role` – Displays the syslog role. • `syslog relay - port` – Sets the syslog port through which it receives the syslog messages • `show syslog relay transport type` – Displays the Syslog relay transport type • `show syslog relay - port` – Displays the Syslog relay port.

11.18 show logging

Command Objective	This command displays all the logging status and configuration information.
Syntax	`show logging`
Mode	Privileged EXEC Mode

Example

```
Your Product# show logging

System Log Information

----------------------

Syslog logging: enabled(Number of messages 0)
Console logging: enabled(Number of messages 1)
TimeStamp option: enabled

Severity logging: Debugging

Log server IP: 10.0.0.1

Facility: Default (local0)

Buffered size: 100 Entries

LogBuffer(0 Entries, 0 bytes)

<129>Aug  7 12:08:02 ISS CLI Attempt to login as root
via console Succeeded
```

Related Command(s)

- `logging` - Enables Syslog Server and configures Syslog Server IP address, log-level and other Syslog related parameter
- `sender mail-id` - Sets the sender mail id from which the email alert messages are sent.

- `cmdbuffs` - Configures the number of syslog buffers for a particular user.
- `clear logs` - Clears the logs buffered in the system.

11.19 show email alerts

Command Objective	This command displays configurations related to email alerts.
Syntax	`show email alerts`
Mode	Privileged EXEC Mode
☞	This command is executed only if mail server is configured.
Example	`Your Product# show email alerts` `Sender email-id: plabinik@Aricent.com`
Related Command(s)	• `mail-server` - Sets the mail server IP address to be used for sending email alert messages • `sender mail-id` - Sets the sender mail id from which the email alert messages are sent.

11.20 show syslog role

Command Objective	This command displays the syslog role.
Syntax	`show syslog role`
Mode	Privileged EXEC Mode
Example	`Your Product# show syslog role` `Syslog Role: Relay`
Related Command(s)	• `syslog relay` - Changes the syslog role from device to relay • `syslog relay transport type` – Sets the syslog relay transport type either as udp or tcp

11.21 show syslog mail

Command Objective	This command displays status of the mail option in syslog.
Syntax	`show syslog mail`
Mode	Privileged EXEC Mode
Example	`Your Product# show syslog mail` `Syslog Mail Option: Enabled`
Related Command(s)	• `syslog mail` – Enables the mail option in syslog

11.22 show syslog localstorage

Command Objective	This command displays the syslog local storage.
Syntax	`show syslog localstorage`
Mode	Privileged EXEC Mode
Example	`Your Product# show syslog localstorage` `Syslog Localstorage: Enabled`

Related Command(s)

- `syslog local storage` – Enables the syslog local storage
- `syslog filename-one` - Configures the first file to store the syslog messages locally
- `syslog filename-two` - Configures the second file name to store the syslog messages locally
- `syslog filename-three`- Configures the third file name to store the syslog messages locally
- `shpw syslog file-name` - Displays all the syslog local storage file names.

11.23 show logging-file

Command Objective	This command displays the priority and file name of all the three files configured in the syslog file table.
Syntax	`show logging-file`
Mode	Privileged EXEC Mode

Example	**`Your Product# show logging-file`**
	`Syslog File Table Information`
	`--------------------------`
	`Priority  File-Name`
	`--------  ----------`
	`134  smis1`
	`134  smis2`
	`134  smis3`

Related Command(s)

- `syslog` - Configures the first file to store the syslog messages locally
- `syslog filename-two` - Configures the second file name to store the syslog messages locally
- `syslog filename-three`- Configures the third file name to store the syslog messages locally
- `logging-file` - Adds an entry in to file table

11.24 show logging-server

Command Objective	This command displays the information about the syslog logging server table.
Syntax	`show logging-server`
Mode	Privileged EXEC Mode

Example	`Your Product# show logging-server`
	`Syslog Forward Table Information`
	`--------------------------------`
	`Priority  Address-Type  IpAddress  Port  Trans-Type`
	`-----  -------  -------  ----  ---`
	`129  ipv4  12.0.0  514  udp`
	`134  ipv4  12.0.0  514  udp`

Related Command(s)	• `logging server` - Adds an entry in to logging-server table

11.25 show mail-server

Command Objective This command displays the information about the syslog mail server table.

Syntax `show mail-server`

Mode Privileged EXEC Mode

Example

```
Your Product# show mail-server

Syslog Mail Table Information

----------------------------

Priority  Address-Type  IpAddress  Receiver Mail-Id          UserName

--------  ------------  ---------  ----------------          ------

5         ipv4          10.10.10.1 support@supermicro.com    JohnD
```

Related Command(s)

- `mail server table` - Adds an entry to mail-server table

11.26 show syslog relay-port

Command Objective	This command displays the Syslog relay port.
Syntax	`show syslog relay-port`
Mode	Privileged EXEC Mode
Example	`Your Product# show syslog relay-port` `Syslog Port: 251`
Related Command(s)	• `syslog relay – port` - Sets the syslog port through which it receives the syslog messages • `syslog relay` – Changes the syslog role from device to relay • `syslog relay transport type` – Sets the syslog relay transport type either as udp or tcp

11.27 show syslog profile

Command Objective	This command displays the syslog profile.
Syntax	`show syslog profile`
Mode	Privileged EXEC Mode
Example	`Your Product# show syslog profile` `Syslog Profile: raw`
Related Command(s)	• `syslog profile` - Sets the profile for reliable syslog

11.28 show syslog relay transport type

Command Objective	This command displays the Syslog relay transport type.
Syntax	`show syslog relay transport type`
Mode	Privileged EXEC Mode
Example	`Your Product# show syslog relay transport type` `Syslog Relay Transport type udp`

Related Command(s)

- `syslog relay transport type` - Sets the Syslog relay transport type either as udp or tcp
- `syslog relay -port` - Sets the syslog port through which it receives the syslog messages
- `syslog relay` – Changes the syslog role from device to relay

11.29 show syslog file-name

Command Objective	This command displays all the syslog local storage file names.
Syntax	`show syslog file-name`
Mode	Privileged EXEC Mode

Example	`Your Product# show syslog file-name`
	`Syslog File Name`
	`----------`
	`Syslog File-One: smis1`
	`Syslog File-Two: smis2`
	`Syslog File-Three: smis3`

Related Command(s)

- `syslog local storage` - Enables the syslog local storage
- `show syslog local storage` - Displays the syslog local storage.
- `syslog filename-one` - Configures the file name to store the syslog messages.
- `syslog filename-two` - Configures the file name to store the syslog messages.
- `syslog filename-three` - Configures the file name to store the syslog messages

11.30 show syslog information

Command Objective	This command displays the status of consolidated syslog log information.
Syntax	`show syslog information`
Mode	Privileged EXEC Mode

Example	`Your Product# show syslog information`
	`System Log Information`
	`----------`
	`Syslog Localstorage: Enabled Syslog`
	`Mail Option: Enabled`
	`Syslog Port: 251`
	`Syslog Role: Relay`
	`Smtp Authentication: None`

Related Command(s)

- `syslog local storage` - Enables the syslog local storage
- `syslog mail` – Enables the mail option in syslog
- `syslog relay` – Changes the syslog role from device to relay
- `smtp authentication` - Sets the smtp authentication method while sending E-mail alerts to the mail server configured

11.31 smtp authentication

Command Objective	This command sets the smtp authentication method while sending E-mail alerts to the mail server configured. The no form of the command resets the authentication method to send email alerts with any authentication

Syntax	`smtp authentication {auth-login | auth-plain | cram-md5 |digest-md5}`
	
	`no smtp authentication`

Parameter **Description**	• `auth-login` - Sets the smtp authentication method as auth-login in which both the user name and password are BASE64 encoded • `auth-plain` - Sets the smtp authentication method as auth-plain in which the user name and password used for authentication are combined to one string and BASE64 encoded. • `cram-md5` - Sends the BASE64 encoded user name and 16-byte digest in hexadecimal notation. The digest is generated using HMAC calculation with password as secret key and SMTP server original challenge as the message. • `digest-md5` - Sets the smtp authentication method as digest-md5 in which the BASE64 encoded MD5 digest response string that is calculated using the user name, password, realm string and nonce string.
Mode	Global Configuration Mode
Example	`Your Product (config)# smtp authentication auth-login`
Related Command(s)	• `show syslog information` – Displays the status of consolidated syslog log information

11.32 snmp trap syslog-server-status

Command Objective	This command enables trap generation when the syslog server is down. The no form of the command disables trap generation when the syslog server is down

Syntax	`snmp trap syslog-server-status`
	
	`no snmp trap syslog-server-status`

Parameter **Description**	• `trap` - Configures trap related parameters. • `syslog-server-status` - Configures syslog server related configurations.
Mode	Global Configuration Mode
Default	Syslog server trap generation is enabled
Example	`Your Product (config)# snmp trap syslog-server-status`

12 TCP

Transmission Control Protocol (TCP) is an implementation of the industry standard TCP based on RFC 793. The software consists of the core

TCP protocol, a library that provides a Socket Layer Interface to support both Telnet Server and HTTP server. TCP interacts with the Network Layer protocols (IPv4/IPv6) and uses their services for end-to-endcommunication.

The list of TCP commands is as follows:

- `show tcp statistics`
- `show tcp connections`
- `show tcp listeners`
- `show tcp retransmission details`
- `tcp max retries`

12.1 show tcp statistics

Command Objective	This command displays the tcp statistics information such as Max connections, Active opens, Passive opens and attempts fail.
Syntax	`show tcp statistics [vrf <vrf-name>]`
Parameter	
Description	`vrf <vrf-name>` - Displays the tcp statistics information for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32 Settings can be configured for the specified VRF through SNMP and when no VRF instance is mentioned the settings are configured for the default VRF
Mode	Privileged EXEC Mode
Example	**Your Product# show tcp statistics** Context Name: default Max Connections: 500 Active Opens: 0 Passive Opens: 0 Attempts Fail: 0 Estab Resets: 0 Current Estab: 0 Input Segments: 0 Output Segments: 0 Retransmitted Segments: 0 Input Errors: 0

```
TCP Segments with RST flag Set: 0

HC Input Segments: 0

HC Output Segments: 0

Context Name: vrf1

Max Connections: 500

Active Opens: 0

Passive Opens: 0

Attempts Fail: 0

Estab Resets: 0

Current Estab: 0

Input Segments: 0

Output Segments: 0

Retransmitted Segments: 0

Input Errors: 0

TCP Segments with RST flag Set: 0

HC Input Segments: 0

HC Output Segments: 0

Context Name: vrf2

Max Connections: 500

Active Opens: 0

Passive Opens: 0

Attempts Fail: 0

Estab Resets: 0

Current Estab: 0

Input Segments: 0

Output Segments: 0

Retransmitted Segments: 0

Input Errors: 0
```

```
TCP Segments with RST flag Set: 0

HC Input Segments: 0

HC Output Segments: 0

Context Name: vrf3

Max Connections: 500

Active Opens: 0

Passive Opens: 0

Attempts Fail: 0

Current Estab: 0

Input Segments: 0

Output Segments: 0

Retransmitted Segments:      0

Input Errors: 0

TCP Segments with RST flag  Set: 0

HC Input Segments: 0

HC Output Segments: 0

Context Name: vrf4

Max Connections: 500

Active Opens: 0

Passive Opens: 0

Attempts Fail: 0

Estab Resets: 0

Current Estab: 0

Input Segments: 0

Output Segments: 0

Retransmitted Segments: 0

Input Errors: 0

TCP Segments with RST flag Set: 0
```

```
HC Input Segments: 0

HC Output Segments: 0

Your Product# show tcp statistics vrf vrf1

Context Name: vrf1

Max Connections: 500

Active Opens: 0

Passive Opens: 0

Attempts Fail: 0

Estab Resets:

Current Estab: 0

Input Segments: 0

Output Segments: 0

Retransmitted Segments: 0

Input Errors: 0

TCP Segments with RST flag Set: 0

HC Input Segments: 0

HC Output Segments: 0
```

12.2 show tcp connections

Command Objective	This command displays the tcp connections for the switch such as Local IP Address type, Local IP, Local Port and Remote Port. It also displays if a connection is TCP MD5 protected and the number of incoming segments that failed MD5 authentication.
Syntax	`show tcp connections [vrf <vrf-name>]`
Parameter	
Description	`vrf <vrf-name>` - Displays the tcp connections for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32
	Connections can be configured for the specified VRF through SNMP and when no VRF instance is mentioned the settings are configured for the default VRF.
Mode	Privileged EXEC Mode

Example	**`Your Product# show tcp connections`**
	`Context Name: default`
	`TCP Connections`
	`==========`
	`Local IP Address Type: IPv4`
	`Local IP: 0.0.0.0`
	`Local Port: 22`
	`Remote IP Address Type: IPv4`
	`Remote IP: 0.0.0.0`
	`Remote Port: 0`

```
TCP State: Listen

MD5 Authenticated: No

TCP Connections

===============

Local IP Address Type: IPv4

Local IP: 0.0.0.0

Local Port: 23

Remote IP Address Type: IPv4

Remote IP: 0.0.0.0

Remote Port: 0

TCP State: Listen

MD5 Authenticated: No

TCP Connections

===============

Local IP Address Type: IPv4

Local IP: 0.0.0.0

Local Port: 80

Remote IP Address Type: IPv4

Remote IP: 0.0.0.0

Remote Port: 0

TCP State: Listen

MD5 Authenticated: No

TCP Connections

===============

Local IP Address Type: IPv4

Local IP: 0.0.0.0

Local Port: 646

Remote IP Address Type: IPv4
```

```
Remote IP: 0.0.0.0

Remote Port: 0

TCP State: Listen

MD5 Authenticated: No

TCP Connections

===============

Local IP Address Type: IPv6

Local IP: ::

Local Port: 22

Remote IP Address Type: IPv6

Remote IP: ::

Remote Port: 0

TCP State: Listen

MD5 Authenticated: No

TCP Connections

===============

Local IP Address Type: IPv6

Local IP: ::

Local Port: 23

Remote IP Address Type: IPv6

Remote IP: ::

Remote Port: 0

TCP State: Listen

MD5 Authenticated: No

TCP Connections

===============

Local IP Address Type: IPv6
```

```
Local IP: ::

Local Port: 80

Remote IP Address Type: IPv6

Remote IP: ::

Remote Port: 0

TCP State: Listen

MD5 Authenticated: No

Context Name: vrf1

Context Name: vrf2

Context Name: vrf3

Context Name: vrf4
```

12.3 show tcp listeners

Command Objective	This command displays the information such as Local IP Address Type, Local IP and Local Port for each listener in the network.
Syntax	`show tcp listeners [vrf <vrf-name>]`
Parameter	
Description	`vrf <vrf-name>` - Displays the TCP listener information for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32 Settings can be configured for the specified VRF through SNMP and when no VRF instance is mentioned the settings are configured for the default VRF
Mode	Privileged EXEC Mode
Example	**Your Product# show tcp listeners** Context Name: default TCP Listeners ========== Local IP Address Type: 0 Local IP: 0.0.0.0 Local Port: 22 Local IP Address Type: 0 Local IP: 0.0.0.0 Local Port: 23 Local IP Address Type: 0 Local IP: 0.0.0.0

```
Local Port: 80

Address Type [0 - IPv4 and IPv6] [1 - IPv4] [2 IPv6]

Context Name: vrf1

Context Name: vrf2

Context Name: vrf3

Context Name: vrf4
```

Your Product# show tcp listeners vrf default

```
Context Name: default

TCP Listeners

===============

Local IP Address Type: 0

Local IP: 0.0.0.0

Local Port: 22

Local IP Address Type: 0

Local IP: 0.0.0.0

Local Port: 23

Local IP Address Type: 0

Local IP: 0.0.0.0

Local Port: 80

Address Type [0 - IPv4 and IPv6] [1 - IPv4] [2 -
IPv6]
```

12.4 show tcp retransmission details

Command Objective	This command displays the tcp retransmission details.
Syntax	`show tcp retransmission details [vrf <vrf-name>]`
Parameter	
Description	`vrf <vrf-name>` - Displays the TCP transmission details for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32
	The retransmission settings can be configured for the specified VRF through SNMP and when no VRF instance is mentioned the settings are configured for the default VRF
Mode	Privileged EXEC Mode
Example	**Your Product# show tcp retransmission details**

```
Context Name: default

RTO Algorithm Used: VAN JACOBSON
Min Retransmission Timeout: 0 msec
Max Retransmission Timeout: 0 msec

Context Name: vrf1

RTO Algorithm Used: VAN JACOBSON
Min Retransmission Timeout: 0 msec
Max Retransmission Timeout: 0 msec

Context Name: vrf2
```

```
RTO Algorithm Used: VAN JACOBSON
Min Retransmission Timeout: 0 msec
Max Retransmission Timeout: 0 msec

Context Name: vrf3

RTO Algorithm Used: VAN JACOBSON
Min Retransmission Timeout: 0 msec
Max Retransmission Timeout: 0 msec

Context Name: vrf4

RTO Algorithm Used: VAN JACOBSON
Min Retransmission Timeout: 0 msec
Max Retransmission Timeout: 0 msec
```

Your Product# show tcp retransmission details vrf default

```
Context Name: default

RTO Algorithm Used: VAN JACOBSON
Min Retransmission Timeout: 0 msec
Max Retransmission Timeout: 0 msec
```

12.5 tcp max retries

Command Objective	This command configures the maximum number of retries for retransmission in TCP module.
Syntax	`tcp max retries {<integer(1-12)>} [vrf <vrf-name>]`
Parameter Description	• `<integer(1-12)>` - Configures the maximum number of retries done by TCP module. This value ranges between 1 and 12. • `vrf <vrf-name>` - Configures the maximum number of retries for re- transmission for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32 When no VRF instance is mentioned the max retries is configured for the default VRF
Mode	Global Configuration Mode
Example	`Your Product (config)# tcp max retries 1`

13 UDP

Aricent UDP (User Datagram Protocol) is an implementation of the industry standard UDP. It is used in packet-switched computer communication networks and in interconnected systems of such networks.

The software consists of the core UDP protocol and a library that provides a Socket Layer Interface for applications like SNMP. It supports a number of standard features in addition to the core protocol.

The following are the list of UDP commands:

- `show udp statistics`
- `show udp connections`

13.1 show udp statistics

Command Objective	This command displays the udp statistics such as InDatagrams, outDatagrams, HC InDatagrams, HC OutDatagrams, UDP No Ports and UDP IN Errors. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
Syntax	`show udp statistics [vrf <vrf-name>]`
Mode	Privileged EXEC Mode
Default	vrf - default

Example	**`Your Product# show udp statistics vrf vr1`**
	`Global UDP Statistics`
	`==========`
	`InDatagrams: 0`
	`OutDatagrams: 0`
	`HC InDatagrams: 0`
	`HC OutDatagrams: 0`
	`UDP No Ports: 4`
	`UDP In Errors: 0`
	`UDP with no Checksum: 0`
	`No. ICMP error packets: 0`
	`UDP with wrong Checksum: 0`
	`UDP In Broadcast Mode: 0`
	`Virtual Context - UDP Statistics`
	`==========`
	`VRF Name: vr1`

```
-----------

InDatagrams:    0

OutDatagrams:    0

HC InDatagrams:  0

HC OutDatagrams: 0

UDP No Ports: 0

UDP In Errors: 0

UDP with no Checksum: 0

No. ICMP error packets: 0

UDP with wrong Checksum: 0

UDP In Broadcast Mode: 0
```

Related Command(s)

- `show udp connections` - Displays the udp configurations for different connections.

13.2 show udp connections

Command Objective	This command displays the udp configurations such as Local IP Address Type, Local IP, Local Port, Remote IP Address Type, Remote IP and Remote Port for various connections.
Syntax	`show udp connections [vrf <vrf-name>]`
Parameter	
Description	• `vrf <vrf-name>` - Displays UDP information for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
Mode	Privileged EXEC Mode

Example	**`Your Product# show udp connections`**
	`Global UDP Connections`
	`========================`
	`Local IP Address Type: 0`
	`Local IP: 0.0.0.0`
	`Local Port: 161`
	`Remote IP Address Type: 0`
	`Remote IP: 0.0.0.0`
	`Remote Port: 0`
	`Local IP Address Type: 0`
	`Local IP: 0.0.0.0`
	`Local Port: 6125`

```
Remote IP Address Type: 0

Remote IP: 0.0.0.0

Remote Port: 0

Local IP Address Type: 0

Local IP: 0.0.0.0

Local Port: 49152

Remote IP Address Type: 0

Remote IP: 0.0.0.0

Remote Port: 0
```

Related Command(s)

- `show udp statistics` - Displays the udp statistics.

14 L2 DHCP Snooping

The DHCP snooping feature filters the untrusted DHCP messages and builds a DHCP snooping binding database. It acts as a firewall between untrusted hosts and DHCP servers. These untrusted messages are sent from devices outside a network and are usually sources of traffic attacks. DHCP snooping binding database maintains a table which contains MAC address, IP address, lease time, binding type, VLAN number and interface information of the local untrusted interfaces of the switch.

The switch uses DHCP option 82 information, relay agent information, to establish the binding datatbase. DHCP server has to support this option and client has to disable this option for the proper operation of DHCP snooping.

The list of CLI commands used to configure the L2 DHCP snooping are:

- `ip dhcp snooping - Global Command`
- `ip dhcp snooping verify mac-address`
- `ip dhcp snooping - VLAN Interface Command`
- `ip dhcp snooping trust`
- `show ip dhcp snooping globals`
- `show ip dhcp snooping vlan`
- `debug ip dhcp snooping`

14.1 ip dhcp snooping - Global Command

Command Objective	This command globally enables the layer 2 DHCP snooping in the switch or enables the snooping in the specific VLAN. The DHCP snooping module will start the protocol operation when the snooping is enabled globally. This value ranges between 1 and 4094. This is a unique value that represents the specific VLAN created. The no form of the command globally disables layer 2 DHCP snooping in the switch or disables DHCP snooping in the specific VLAN. The DHCP snooping module will stop the protocol operation when the snooping is globally disabled.

Syntax	`ip dhcp snooping [ vlan < vlan-id (1-4094)>]`
	
	`no ip dhcp snooping [vlan <integer(1-4094)>]`

Mode	Global Configuration mode
Default	DHCP snooping is globally disabled in the switch and on all VLAN's.
☞	The Example used and the ip dhcp snooping command used in the config-vlan mode serve the same purpose.
Example	`Your Product (config)# ip dhcp snooping vlan 2`
Related Command(s)	• `show ip dhcp snooping globals` - Displays the global configuration of dhcp snooping • `show ip dhcp snooping vlan` - Displays the configuration and statistics of the specified VLAN

14.2 ip dhcp snooping verify mac-address

Command Objective	This command globally enables DHCP MAC verification in the switch. The no form of the command globally disables DHCP MAC verification in the switch. If the MAC verification status is enabled, DHCP snooping module will verify whether the source Mac address and client hardware Mac address are same. If they are same, packet will be processed further, else, it is dropped.

Syntax	`ip dhcp snooping verify mac-address`
	
	`no ip dhcp snooping verify mac-address`

Mode	Global Configuration Mode
Default	DHCP MAC address verification is enabled.
Example	`Your Product (config)# ip dhcp snooping verify mac-address`
Related Command(s)	• `show ip dhcp snooping globals` - Displays the global configuration of dhcp snooping

14.3 ip dhcp snooping - VLAN Interface Command

Command Objective	This command enables layer 2 DHCP snooping in the VLAN. The no form of the command disables layer 2 DHCP snooping in the VLAN. DHCP snooping feature filters the untrusted DHCP messages to provide security for DHCP servers.

Syntax	`ip dhcp snooping`
	
	`no ip dhcp snooping`

Mode	Config-VLAN mode
Default	L2 DHCP snooping is disabled on VLANs
Example	`Your Product (config-vlan)# ip dhcp snooping`
Related Command(s)	• `show ip dhcp snooping vlan` – displays the configuration and statistics of the specified VLAN • `ip dhcp snooping – Global command` – This command enables layer 2 dhcp snooping on a particular VLAN.

14.4 ip dhcp snooping trust

Command Objective	This command configures the port as a trusted port. The no form of the command configures the port as an untrusted port. The packets coming from the trusted port is considered as trusted packets and are not filtered by the DHCP snooping feature.
Syntax	`ip dhcp snooping trust` `no ip dhcp snooping trust`
Mode	Interface Configuration mode
Default	Ports are considered as trusted
Example	`Your Product (config-if)# ip dhcp snooping trust`

14.5 show ip dhcp snooping globals

Command Objective	This command displays the global configuration of DHCP snooping. The global status of layer 2 DHCP snooping and MAC verification are displayed.
Syntax	`show ip dhcp snooping globals [switch <Context Name>]`
Parameter	
Description	• `switch<Context Name>` - Displays the global configuration of DHCP snooping for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to MI feature.
Mode	Privileged EXEC mode

Example	`Your Product# show ip dhcp snooping globals`
	`DHCP Snooping Global information`
	`--------------------------------`
	`Layer 2 DHCP Snooping is globally disabled`
	`MAC Address verification is enabled`

Related Command(s)	• `ip dhcp snooping – Global command` - Globally enables the layer 2 DHCP snooping in the switch and allocates the resources for the DHCP snooping module. • `ip dhcp snooping verify mac-address` - Globally enables DHCP MAC verification in the switch.

14.6 show ip dhcp snooping vlan

Command Objective	This command displays the DHCP snooping configuration and statistics of all VLANs in which the DHCP snooping feature is enabled.
Syntax	`show ip dhcp snooping [vlan <vlan-id (1-4094)>] [switch <context name>]`
Parameter Description	• `vlan <vlan-id (1-4094)>` - Displays the DHCP snooping configuration and statistics for the specified VLAN ID. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094. • `switch<context name>` - Displays the DHCP snooping configuration and statistics for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to MI feature.
Mode	Privileged EXEC mode

Example	**`Your Product# show ip dhcp snooping vlan 3`**
	`DHCP Snooping Vlan information`
	`----------`
	`VLAN: 3`
	`Snooping status: Enabled`
	`Number of Incoming Discovers: 0`
	`Number of Incoming Requests: 0`
	`Number of Incoming Releases: 0`
	`Number of Incoming Declines: 0`
	`Number of Incoming Informs: 0`

```
Number of Transmitted Offers: 0

Number of Transmitted Acks: 0

Number of Transmitted Naks: 0

Total Number Of Discards: 0

Number of MAC Discards: 0

Number of Server Discards: 0

Number of Option Discards: 0
```

Related Command(s)

- **`ip dhcp snooping - VLAN interface command`** - Enables layer 2 DHCP snooping in the VLAN.

14.7 debug ip dhcp snooping

Command Objective	This command enables the tracing of the DHCP snooping module as per the configured debug level. The trace statements are generated for the configured trace levels. The no form of the command disables the tracing of the DHCP module. The trace statements are not generated for the configured trace levels. This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command.

Syntax	`debug ip dhcp snooping {[entry][exit][debug][fail] | all}`
	
	`no debug ip dhcp snooping`

Parameter **Description**	• `entry` - Generates debug statements for function entry traces. The names of the functions entered are displayed in the log. • `exit` - Generates debug statements for function exit traces. The names of the functions exited are displayed in the log. • `debug` - Generates debug statements for debug traces. This is used for debugging the packet flow of DHCP snooping functionality. • `fail` - Generates debug statements for all failure traces. These traces are used for all valid and invalid failures. The valid failures represent the expected error. The invalid failures represent the unexpected error. • `all` - Generates debug statements for all types of traces.
Mode	Privileged EXEC mode
Example	`Your Product# debug ip dhcp snooping entry`

15 IPDB

IP source guard is used to restrict the IP traffic on Layer 2 interfaces by filtering traffic based on the IP binding database.

The list of CLI commands for the configuration of IPDB is as follows:

- `ip binding`
- `ip source binding`
- `ip verify source`
- `show ip binding`
- `show ip source binding`
- `show ip binding counters`
- `show ip verify source`
- `debug ip binding database`

15.1 ip binding

Command Objective

This command configures the static binding information for the hosts connected to the switch.

The no form of the command deletes the binding information for the specified host.

Syntax

```
ip binding <mac-address> vlan <vlan-id (1-4094)>
<ip address> interface <interface-type>
<interface-id> gateway <ip address>

no ip binding <mac-address> vlan <vlan-id (1-4094)>
```

Parameter

Description

- `<mac-address>` - Configures the unicast MAC address of the host for which the binding information should be configured.
- `<vlan-id (1-4094)>` - Configures the VLAN ID to which the host belongs. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
- `<ip address>` - Configures IP address of the host for which the binding information should be configured.
- `<interface-type>` - Configures the type of interface to which the host is connected. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Configures the interface identifier to which the host is connected. This is a unique value that represents the specific interface.
  - This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1.

- **gateway <ip address>** - Configures the IP address of the gateways to which the host has access.

Mode	Global Configuration mode

Example

```
Your Product (config)# ip binding 00:01:02:03:04:05
vlan 330.0.0.4 interface gigabitethernet 0/2 gateway
30.0.0.1
```

Related Command(s)

- **show ip binding** - Displays the IP binding database.
- **show ip binding counters** - Displays the global or VLAN statistics information.

15.2 ip source binding

Command Objective

This command adds a static IP source binding entry.

The no form of the command deletes the static IP source binding entry.

Syntax

```
ip source binding <mac-address> vlan <vlan-id (1-4094)> <ip-address> interface <interface-type> <interface-id> [gateway <gateway-ip>]
```

```
no ip source binding <mac-address> vlan <vlan-id (1-4094)> <ip-address> interface <interface-type> <interface-id>
```

Parameter Description

- `<mac-address>` - Configures the unicast MAC address of the host for which the binding information should be configured.
- `<vlan-id (1-4094)>` - Configures the VLAN ID to which the host belongs. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
- `<ip-address>` - Configures IP address of the host for which the binding information should be configured.
- `<interface-type>` - Configures the type of interface to which the host is connected. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer upto
  - 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Configures the interface identifier to which the host is connected. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1.

- `gateway <gateway-ip>` - Configures the gateway IP address of the gateways to which the host has access.

Mode	Global Configuration mode
Example	Your Product (config)# ip source binding 00:01:02:03:04:05 vlan 3 30.0.0.4 interface gigabitethernet 0/2 gateway 30.0.0.1

Related Command(s)

- `show ip source binding` - Displays the source IP binding database.

15.3 ip verify source

Command Objective	This command enables the IP source guard status for the specified interface. The no form of the command disables the IP source guard on an interface. The port-security option is mandatory for this command. Else the following error message gets displayed 'IP source guard feature does not support source IP filter type.

Syntax	`ip verify source [ port-security ]`
	
	`no ip verify source [ port-security ]`

Mode	Interface Configuration Mode
Default	Disable
Example	`Your Product (config-if)# ip verify source port-security`
Related Command(s)	• `show ip verify source` - Displays the IP source guard interface status.

15.4 show ip binding

Command Objective This command displays the IP binding database.

Syntax

```
show ip binding [vlan <vlan-id (1-4094)>] {[ static | dhcp | ppp ]} [switch <switch_name>]
```

Parameter

Description

- vlan <vlan-id (1-4094)> - Displays the VLAN ID to which the host belongs. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
- static - Displays the static ip binding configuration.
- dhcp - Displays the dynamic IP binding updates through DHCP snooping.
- ppp - Displays the dynamic IP binding updates through Pppoe intermediate agent.
- switch <switch_name> - Displays the database of the specified switch.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip binding vlan 2 static
Host Binding Information
------------------------
VLAN  HostMac           HostIP    Port   GatewayIP  Type
----  ----------------  --------  ----  ----------  -----
2     00:10:12:13:13:15  12.0.0.1  Gi0/1   12.0.0.0 static
```

Related Command(s)

- ip binding – Configures the static binding information for the hosts connected to the switch.

15.5 show ip source binding

Command Objective This Command displays the source IP binding database.

Syntax

```
show ip source binding [<ip-address>] [<mac-address>] [{dhcp-snooping | static }] [ interface <interface-type> <interface-id> ] [ vlan <vlan-id (1-4094)> ] [switch <switch_name>]
```

Parameter

Description

- `<ip-address>` - Displays the IP address of the host for which the binding information should be configured.
- `<mac-address>` - Displays the unicast MAC address of the host for which the binding information should be configured.
- `dhcp-snooping` - Displays the dynamic IP binding updation through DHCP snooping.
- `static` - Displays the static ip binding configuration.
- `<interface-type>` - Displays the type of interface to which the host is connected. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Displays the interface identifier to which the host is connected. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1.
- `vlan <vlan-id (1-4094)>` - Displays the VLAN ID to which the host belongs. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
- `switch <switch_name>` - Displays the status of the ip source binding of the specified switch.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip source binding
Host Binding Information
------------------------
VLAN     HostMac     HostIP     Port     GatewayIP Type
-----  ------------ --------- ---------- ------------ --
```

Related Command(s)

- `ip source binding` - Adds a static IP source binding entry

15.6 show ip binding counters

Command Objective This command displays the global or VLAN statistics information.

Syntax

```
show ip binding counters [{[vlan <short (1-4094)>] |
global | [ switch <switch-name>] }]
```

Parameter Description

- `vlan <short (1-4094)>` - Displays the VLAN ID to which the host belongs. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
- `global` - Displays the static information of all binding types (static, dhcp, ppp)
- `switch <switch-name>` - Displays the static information of the specified VLAN.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip binding counters vlan 2
Global Binding count Information
-----------------------------
Number of Bindings: 1
Number of Static Bindings: 1
Number of DHCP Bindings: 0
Number of PPP Bindings: 0
```

Related Command(s)

- `ip binding` - Configures the static binding information for the hosts connected to the switch.

15.7 show ip verify source

Command Objective	This command displays the IP source guard interface status.
Syntax	`show ip verify source [ interface <interface-type> <interface-id> ]`
Parameter	
Description	• `<interface-type>` - Displays the type of interface to which the host is connected. The interface can be: – qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links. – gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. – extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. – port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. • `<interface-id>` - Configures the interface identifier to which the host is connected. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1.
Mode	Privileged EXEC Mode

Example	`Your Product# show ip verify source`
	`Interface IP Source guard Status`
	`--------- ----------------------`
	`Gi0/1 Disable`
	`Gi0/2 Disable`

```
Gi0/3          Disable
Gi0/4          Disable
Gi0/5          Disable
Gi0/6          Disable
Gi0/7          Disable
Gi0/8          Disable
Gi0/9          Disable
Gi0/10         Disable
Gi0/11         Disable
Gi0/12         Disable
Gi0/13         Disable
Gi0/14         Disable
Gi0/15         Disable
Gi0/16         Disable
Gi0/17         Disable
Gi0/18         Disable
Gi0/19         Disable
Gi0/20         Disable
Gi0/21         Disable
Gi0/22         Disable
Gi0/23         Disable
Gi0/24         Disable
```

Related Command(s)

- `ip verify source` - Enables the IP source guard status for the specified interface

15.8 debug ip binding database

Command Objective	This command specifies the debug levels for IP Binding Database module. The no form of this command disables IPDB module debugging.

Syntax	`debug ip binding database {[entry][exit][debug][fail] |all}`
	
	`no debug ip binding database [{ [entry][exit][debug][fail]| all }]`

Parameter **Description**	• `entry` - Generates debug statements for all function entry traces. • `exit` - Generates debug statements for all function exit traces. • `debug` - Generates debug statements for all debug traces. • `fail` - Generates debug statements for all the failure traces. • `all` - Generates debug statements for all the above-mentioned traces.
Mode	Privileged EXEC Mode
Example	`Your Product# debug ip binding database entry`

16 STP

STP (Spanning-Tree Protocol) is a link management protocol that provides path redundancy while preventing undesirable loops in the network that are created by multiple active paths between stations. To establish path redundancy, STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby or blocked state.

For an Ethernet network to function properly, only one active path should exist between two stations. Multiple active paths between stations in a bridged network can cause loops in which Ethernet frames can endlessly circulate. STP logically breaks such loops and prevents looping traffic from clogging the network. The dynamic control of the topology provides continued network operation in the presence of redundant or unintended looping paths.

The list of CLI commands for the configuration of STP is common to both SI and MI except for a difference in the prompt that appears for the switch with MI support. The prompt for the switch configuration Mode is,

```
Your Product(config-switch)# spanning-tree Mode rst
```

The STP functionality is realized in the network using one of the following STPs:

- RSTP
- MSTP

16.1 STP Commands Common for RSTP and MSTP

This section describes all spanning tree protocol Related Commands that are common for all kinds of STPs.

RSTP

SMIS RSTP is an implementation of the IEEE 802.1D standard. It provides rapid recovery of connectivity following the failure of a bridge/bridge port or a LAN. It reduces the time to reconfigure the active topology of the network when physical topology or topology configuration parameters changes. It provides increased availability of MAC service when there is a reconfiguration or failure of components in a bridged LAN. It can interoperate with legacy STP bridges without any change in the configuration.

The list of common STP commands for the configuration of STP (RSTP / MSTP) is as follows:

- shutdown spanning-tree
- spanning-tree
- spanning-tree Mode
- spanning-tree compatibility
- spanning-tree timers
- spanning-tree transmit hold-count
- clear spanning-tree counters
- spanning-tree pathcost dynamic
- spanning-tree priority
- spanning-tree auto-edge
- spanning-tree - Properties of an interface
- spanning-tree portfast - disable | trunk
- spanning-tree portfast - bpdufilter default | bpduguarddefault | default
- spanning-tree restricted-role
- spanning-tree restricted-tcn
- spanning-tree layer2-gateway-port
- spanning-tree bpdu-receive
- spanning-tree bpdu-transmit
- spanning-tree loop-guard
- spanning-tree – Pseudoroot configuration
- debug spanning-tree
- clear spanning-tree detected protocols
- show spanning-tree - Summary, Blockedports, Pathcost, Redundancy
- show spanning-tree detail
- show spanning-tree active
- show spanning-tree interface
- show spanning-tree root

- show spanning-tree bridge
- show spanning-tree – layer 2 gateway port
- show customer spanning-tree
- spanning-tree forwarddelay optimization alternate-role

16.2 shutdown spanning-tree

Command Objective	This command shuts down spanning tree functionality in the switch. The switch does not execute any kind of STP to form a loop free topology in the Ethernet network and operates with the existing topology structure.
Syntax	`shutdown spanning-tree`
Mode	Global Configuration Mode
Default	Spanning tree MSTP is started and enabled in the switch.
Example	`Your Product(config)# shutdown spanning-tree`

Related Command(s)

- `base bridge-Mode` - Configures the base Mode (either 802.1d transparent bridge Mode or 802.1q vlan aware bridge Mode) in which the VLAN feature should operate on the switch.
- `spanning-tree` - Enables the spanning tree operation in the switch for the selected spanning tree Mode.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree compatibility` - Sets the STP compatibility version in the switch for all ports.
- `spanning-tree timers` - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- `spanning-tree transmit hold-count` - Sets the transmit hold-count value for the switch.
- `clear spanning-tree counters` - Deletes all bridge and port level spanning tree statistics information.
- `spanning-tree pathcost dynamic` - Enables dynamic pathcost calculation feature in the switch.

- **spanning-tree priority** - Configures the priority value that is assigned to the switch.
- **spanning-tree auto-edge** - Enables automatic detection of Edge port parameter of an interface.
- **spanning-tree - Properties of an interface** - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- **spanning-tree restricted-role** - Enables the restricted role feature for a port.
- **spanning-tree restricted-tcn** - Enables the topology change guard / restricted TCN feature on a port.
- **spanning-tree layer2-gateway-port** - Configures a port to operate as a L2GP.
- **spanning-tree bpdu-receive** - Configures the processing status of the BPDUs received in a port.
- **spanning-tree bpdu-transmit** - Configures the BPDU transmission status of a port.
- **spanning-tree loop-guard** - Enables the loop guard feature in a port.
- **spanning-tree – Pseudoroot configuration** - Configures the pseudoroot related information for a port set as L2GP.
- **show spanning-tree - Summary, Blockedports, Pathcost,** redundancy - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- **show spanning-tree detail** - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- **show spanning-tree active** - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- **show spanning-tree interface** - Displays the port related spanning tree information for the specified interface.
- **show spanning-tree root** - Displays the spanning tree root information.
- **show spanning-tree bridge** - Displays the spanning tree bridge information.
- **show spanning-tree – layer 2 gateway port** - Displays spanning tree information for all L2GPs enabled in the switch.
- **spanning-tree mst max-hops** - Configures the maximum number of hops permitted in the MST.
- **spanning-tree mst configuration** - Enters into MST configuration Mode, where instance specific and MST region configuration can be done.

- **spanning-tree mst max-instance** - Configures the maximum number of active MSTIs that can be created.
- **spanning-tree mst- Properties of an interface for MSTP** - Configures the port related spanning tree information for a specified MSTI.
- **spanning-tree mst hello-time** - Configures the hello time for an interface that is enabled.
- **show spanning-tree mst - CIST or specified mst Instance** - Displays multiple spanning tree information for all MSTIs in the switch.
- **show spanning-tree mst configuration** - Displays multiple spanning tree instance related information.
- **show spanning-tree mst - Port Specific Configuration** - Displays multiple spanning tree port specific information for the specified port.
- **spanning-tree vlan** - Configures spanning tree related information on a per VLAN basis.
- **spanning-tree bpduguard** - Configures the status of BPDU guard feature in an interface.
- **spanning-tree guard** - Configures the various PVRST guard features such as root guard, in a port.
- **spanning-tree encap** - Configures the encapsulation type to be used in an interface.
- **spanning-tree vlan status** - Configures the status of PVRST on a port for the specified VLAN.
- **spanning-tree vlan port-priority** - Configures the priority of a port for the specified VLAN.
- **spanning-tree vlan cost** - Configures the cost of a port for the specified VLAN.
- **show spanning-tree vlan - Summary, Blockedports, Pathcost** - Displays PVRST related information for the specified VLAN.
- **show spanning-tree vlan - bridge** - Displays the PVRT related information of the bridge for the specified VLAN ID.
- **show spanning-tree vlan - root** - Displays the PVRT related information of the root, for the specified VLAN ID.
- **show spanning-tree vlan - interface** - Displays interface specific PVRST information for the specified VLAN.

16.3 spanning-tree

Command Objective	This command enables the spanning tree operation in the switch for the selected spanning tree Mode. Spanning tree operation provides path redundancy while preventing undesirable loops in the network that are created by multiple active paths between stations. It logically breaks such loops and prevents looping traffic from clogging the network. The no form of this command disables the spanning tree operation in the switch. The spanning tree operation is automatically enabled in the switch, once the spanning tree Mode is changed.

Syntax	`spanning-tree`
	
	`no spanning-tree`

Mode	Global Configuration Mode
Default	Spanning tree MSTP is started and enabled in the switch.
☞	The spanning tree operation can be enabled in the switch only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.
Example	`Your Product(config)#spanning-tree`
Related Command(s)	• `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.

- **spanning-tree Mode** - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- **show spanning-tree - Summary, Blockedports, Pathcost, redundancy** - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- **show spanning-tree detail** - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- **show spanning-tree active** - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- **show spanning-tree interface** - Displays the port related spanning tree information for the specified interface.
- **show spanning-tree bridge** - Displays the spanning tree bridge information.
- **show spanning-tree mst - CIST or specified mst Instance** - Displays multiple spanning tree information for all MSTIs in the switch.
- **show spanning-tree mst - Port Specific Configuration** - Displays multiple spanning tree port specific information for the specified port.
- **show spanning-tree vlan - Summary, Blockedports, Pathcost** - Displays PVRST related information for the specified VLAN.
- **show spanning-tree vlan - interface** - Displays interface specific PVRST information for the specified VLAN.

16.4 spanning-tree Mode

Command Objective	This command sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch. The current selected type of spanning tree is enabled and the existing spanning tree type is disabled in the switch.
Syntax	`spanning-tree Mode {mst|rst}` `no spanning-tree Mode`
Parameter	
Description	• `mst` - Configures the switch to execute MSTP for preventing undesirable loops. MSTP configures spanning tree on per VLAN basis or multiple VLANs per spanning tree. The Mode cannot be set as mst, if the base bridge Mode is configured as transparent bridging. • `rst` - Configures the switch to execute RSTP for preventing undesirable loops. RSTP provides rapid recovery of connectivity following the failure of a bridge/bridge port or a LAN.
Mode	Global Configuration Mode
Default	mst
Example	Your Product(config)#spanning-tree Mode rst
Related Command(s)	• `base bridge-Mode` - Configures the base Mode (either 802.1d transparent bridge Mode or 802.1q vlan aware bridge Mode) in which the VLAN feature should operate on the switch. • `set gvrp disable` – Globally disables GVRP feature on all ports of a switch.

- **shutdown spanning-tree** - Shuts down spanning tree functionality in the switch.
- **spanning-tree** - Enables the spanning tree operation in the switch for the selected spanning tree Mode.
- **spanning-tree compatibility** - Sets the STP compatibility version in the switch for all ports.
- **spanning-tree timers** - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- **spanning-tree transmit hold-count** - Sets the transmit hold-count value for the switch.
- **clear spanning-tree counters** - Deletes all bridge and port level spanning tree statistics information.
- **spanning-tree pathcost dynamic** - Enables dynamic pathcost calculation feature in the switch.
- **spanning-tree priority** - Configures the priority value that is assigned to the switch.
- **spanning-tree auto-edge** - Enables automatic detection of Edge port parameter of an interface.
- **spanning-tree - Properties of an interface** - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- **spanning-tree restricted-role** - Enables the restricted role feature for a port.
- **spanning-tree restricted-tcn** - Enables the topology change guard / restricted TCN feature on a port.
- **spanning-tree layer2-gateway-port** - Configures a port to operate as a L2GP.
- **spanning-tree bpdu-receive** - Configures the processing status of the BPDUs received in a port.
- **spanning-tree bpdu-transmit** - Configures the BPDU transmission status of a port.
- **spanning-tree loop-guard** - Enables the loop guard feature in a port.
- **spanning-tree – Pseudoroot configuration** - Configures the pseudoroot related information for a port set as L2GP.
- **show spanning-tree - Summary, Blockedports, Pathcost, redundancy** - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- **show spanning-tree detail** - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.

- **show spanning-tree active** - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- **show spanning-tree interface** - Displays the port related spanning tree information for the specified interface.
- **show spanning-tree root** - Displays the spanning tree root information.
- **show spanning-tree bridge** - Displays the spanning tree bridge information.
- **show spanning-tree – layer 2 gateway port** - Displays spanning tree information for all L2GPs enabled in the switch.
- **spanning-tree mst max-hops** - Configures the maximum number of hops permitted in the MST.
- **spanning-tree mst max-instance** - Configures the maximum number of active MSTIs that can be created.
- **spanning-tree mst configuration** - Enters into MST configuration Mode, where instance specific and MST region configuration can be done.
- **spanning-tree mst- Properties of an interface for MSTP** - Configures the port related spanning tree information for a specified MSTI.
- **spanning-tree mst hello-time** - Configures the hello time for an interface that is enabled.
- **show spanning-tree mst - CIST or specified mst Instance** - Displays multiple spanning tree information for all MSTIs in the switch.
- **show spanning-tree mst configuration** - Displays multiple spanning tree instance related information.
- **show spanning-tree mst - Port Specific Configuration** - Displays multiple spanning tree port specific information for the specified port.
- **spanning-tree vlan** - Configures spanning tree related information on a per VLAN basis.
- **spanning-tree bpduguard** - Configures the status of BPDU guard feature in an interface.
- **spanning-tree guard** - Configures the various PVRST guard features such as root guard, in a port.
- **spanning-tree encap** - Configures the encapsulation type to be used in an interface.
- **spanning-tree vlan status** - Configures the status of PVRST on a port for the specified VLAN.
- **spanning-tree vlan port-priority** - Configures the priority of a port for the specified VLAN.

- **spanning-tree vlan cost** - Configures the cost of a port for the specified VLAN.
- **show spanning-tree vlan - Summary, Blockedports, Pathcost** - Displays PVRST related information for the specified VLAN.
- **show spanning-tree vlan - bridge** - Displays the PVRT related information of the bridge for the specified VLAN ID.
- **show spanning-tree vlan - root** - Displays the PVRT related information of the root, for the specified VLAN ID.
- **show spanning-tree vlan - interface** - Displays interface specific PVRST information for the specified VLAN.
- **spanning-tree flush-interval** - Configures the flush interval timer value
- **spanning-tree flush-indication-threshold** – Configures the flush indication threshold value for a specific instance.
- **spanning-tree forwarddelay optimization alternate-role** - Enables and disables the optimization for spanning-tree related protocol in alternate port role transition.

16.5 spanning-tree compatibility

Command Objective

This command sets the STP compatibility version in the switch for all ports.

The no form of this command sets the STP compatibility version to its default value. The STP compatibility version is changed to its default value even if the spanning tree Mode is changed.

The compatibility version allows the switch to temporarily operate (that is, till this configuration is reset manually) in other STP version even though the spanning tree Mode is set as some other version. This configuration is useful during cases where spanning tree Mode itself is not required to be changed.

Syntax

```
spanning-tree compatibility {stp|rst|mst}
```

Parameter

Description

- `stp` - Configures the switch to execute spanning tree operation as specified in IEEE 802.1D.
- `rst` - Configures the switch to execute spanning tree operation as specified in IEEE 802.1w.
- `mst` - Configures the switch to execute spanning tree operation as specified in IEEE 802.1s. The STP compatibility version cannot be set as mst, if the spanning tree Mode is set as rst.

Mode

Global Configuration Mode

Default

If STP Mode is set as mst, then spanning tree compatibility is set as mst.

The STP compatibility version can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

The STP compatibility version does not change the operation of the switch whose spanning tree Mode is set as PVRST.

Example Your Product(config)#spanning-tree compatibility stp

Related Command(s)

- **shutdown spanning-tree** - Shuts down spanning tree functionality in the switch.
- **spanning-tree Mode** - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- **show spanning-tree - Summary, Blockedports, Pathcost,Redundancy** - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- **show spanning-tree detail** - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- **show spanning-tree active** - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- **show spanning-tree vlan - Summary, Blockedports, Pathcost** - Displays PVRST related information for the specified VLAN.

16.6 spanning-tree timers

Command Objective	This command sets the spanning tree timers such as hello time used for controlling the transmission of BPDUs during the computation of loop free topology. The no form of this command resets the spanning tree timers to its default values. The spanning tree timers are reset to its default value, even if the spanning tree Mode is changed.

Syntax	`spanning-tree {forward-time <seconds(4-30)> | hello-time <seconds(1-2)> | max-age <seconds(6-40)>}`
	
	`no spanning-tree { forward-time | hello-time | max-age }`

Parameter **Description**	• `forward-time` - Configures the number of seconds, a port waits before changing from the blocking state to the forwarding state. This value ranges between 4 and 30 seconds. In MSTP, this time configuration is applied for IST root (that is, MSTI 0). • `hello-time` - Configures the time interval (in seconds) between two successive configuration BPDUs generated by the root switch. This value should be either 1 or 2 seconds. This value is configured on per-port basis for MSTP and is configured globally for RSTP. • `max-age` - Configures the maximum expected arrival time (in seconds) of hello BPDUs. STP information learned from network on any port is discarded, once the configured arrival time expires. The spanning tree topology is re-computed after this time interval. This value ranges between • 6 and 40 seconds. In MSTP, this time configuration is applied for IST root (that is, MSTI 0).
	Spanning-tree timers can be configured in centi seconds through SNMP
Mode	Global Configuration Mode

Default

- forward-time - 15 seconds
- hello-time - 2 seconds
- max-age - 20 seconds

The values configured for the spanning tree timers should satisfy the following conditions:

2 * (forward-time - 1) >= max-age, and max-age >= 2 * (hello-time +1)

The STP timers can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

This spanning tree timer's configuration is not supported in PVRST Mode.

Example

```
Your Product(config)#spanning-tree max-age 6
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `show spanning-tree - Summary, Blockedports, Pathcost, Redundancy` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree interface detail` - Displays detailed spanning tree related information for the specified port.
- `show spanning-tree root` - Displays the spanning tree root information.
- `show spanning-tree bridge` - Displays the spanning tree bridge information.
- `show spanning-tree mst - CIST or specified mst Instance` - Displays multiple spanning tree information for all MSTIs in the switch.

- **`show spanning-tree mst - Port Specific Configuration`** - Displays multiple spanning tree port specific information for the specified port.

16.7 spanning-tree transmit hold-count

Command Objective	This command sets the BPDU transmit hold-count value for the switch. The transmit hold count value is a counter that is used to limit the maximum BPDU transmission rate of the switch and to avoid flooding. This value specifies the maximum number of BPDU packets that can be sent in a given hello time interval. This value ranges between 1 and 10. The no form of this command sets the transmit hold-count to its default value. The transmit hold-count is changed to its default value even if the spanning tree Mode is changed.

Syntax	`spanning-tree transmit hold-count <value (1-10)>`
	
	`no spanning-tree transmit hold-count`

Mode	Global Configuration Mode
Default	6, if the spanning tree Mode is set as mst. 3, if the spanning tree Mode is set as rst or pvrst.
☞	The transmit hold-count value can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown. This transmit hold count value configuration is not supported in PVRST Mode.
Example	`Your Product(config)#spanning-tree transmit hold-count 5`
Related Command(s)	• `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.

- **spanning-tree Mode** - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- **show spanning-tree detail** - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- **show spanning-tree active detail** - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- **show spanning-tree vlan - Summary, Blockedports, Pathcost** - Displays PVRST related information for the specified VLAN.

16.8 clear spanning-tree counters

Command Objective

This command deletes all bridge and port level spanning tree statistics information.

For RSTP, the information contains number of:

- Transitions to forwarding state
- RSTP BPDU count received / transmitted
- Config BPDU count received / transmitted
- TCN BPDU count received / transmitted
- Invalid BPDU count transmitted
- Port protocol migration count

For MSTP, the information contains number of:

- Port forward transitions
- Port received BPDUs
- Port transmitted BPDUs
- Port invalid BPDUs received
- Port protocol migration count
- BPDUs sent / received for each MSTI and 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs. This option is applicable, only if the spanning tree Mode is set as mst.

Parameter

Description

- `interface` - Clears all port-level spanning-tree statistics information for the given port.
- `<interface-type>` -Clears all port-level spanning-tree statistics information for the specified type of interface. The interface can be:
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.

- **<interface-id>** – Clears all port-level spanning-tree statistics information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel.

For Example: 0/1 representsthat the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface types port-channel. For Example: 1 represents port-channel ID.

Global Configuration Mode

☞ The statistics information can be deleted, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example

```
Your Product(config)# clear spanning-tree mst 1
counters
```

Related Command(s)

- **shutdown spanning-tree** - Shuts down spanning tree functionality in the switch.
- **spanning-tree Mode** - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- **instance** - Creates an MST instance and maps it to VLANs.
- **show spanning-tree detail** - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- **show spanning-tree active detail** - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- **show spanning-tree interface** - Displays the port related spanning tree information for the specified interface.
- **show spanning-tree mst - CIST or specified mst Instance** - Displays multiple spanning tree information for all MSTIs in the switch.
- **show spanning-tree mst - Port Specific Configuration** - Displays multiple spanning tree port specific information for the specified port.

- **`show spanning-tree vlan - Summary, Blockedports, Pathcost`** - Displays PVRST related information for the specified VLAN.
- **`show spanning-tree vlan - interface`** - Displays interface specific PVRST information for the specified VLAN.

16.9 spanning-tree pathcost dynamic

Command Objective	This command enables dynamic pathcost calculation feature in the switch. The no form of this command disables dynamic pathcost calculation feature in the switch. The dynamic pathcost calculation feature is disabled, even if the spanning tree Mode is changed. The path cost of the port / MSTI is dynamically calculated. This feature is applied only for the ports that are not shutdown during the execution of STP. The calculated path cost is not changed based on the operational status of the port / for a MSTI, once calculated. The manually assigned / already calculated path cost is used even if the dynamic pathcost calculation feature is enabled in the switch.

Syntax	`spanning-tree pathcost dynamic [lag-speed]`
	
	`no spanning-tree pathcost dynamic [lag-speed]`

Parameter **Description**	• `lag speed` - Calculates the path cost for change in speed of the port. This feature is used for LA ports whose speed changes due to addition or deletion of ports from the port channel. The manually assigned path cost is used even if the lag speed feature is enabled in the switch, if the path cost is assigned manually. The lag speed feature can be enabled, only after enabling the dynamic pathcost calculation feature.
Mode	Global Configuration Mode
Default	Dynamic pathcost calculation feature is disabled in the switch.

☞ The dynamic pathcost calculation feature can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example

```
Your Product(config)# spanning-tree pathcost dynamic
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree - Properties of an interface` - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- `show spanning-tree - Summary, Blockedports, Pathcost, Redundancy` – Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `spanning-tree mst- Properties of an interface for MSTP` - Configures the port related spanning tree information for a specified MSTI.
- `spanning-tree vlan cost` - Configures the cost of a port for the specified VLAN.

16.10 spanning-tree priority

Command Objective	This command configures the priority value that is assigned to the switch. The no form of this command resets the priority to its default value. The priority value is changed to its default value even if the spanning tree Mode is changed. In RSTP, this value is used during the election of root. In MSTP, this value is used during the election of CIST root, CIST regional root and IST root.

Syntax	`spanning-tree [mst <instance-id>] priority <value(0-61440)>`
	
	`no spanning-tree [mst <instance-id(1-64)>] priority`

Parameter **Description**	• `mst <instance-id>` - Configures the ID of MSTP instance already created in the switch. This value ranges between 1 and 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs. This option is applicable, only if the spanning tree Mode is set as mst. • `priority <value(0-61440)>` - Configures the priority value for the switch and for the MSTI, in RSTP and MSTP respectively. This value ranges between 0 and 61440. The value should be set in steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288 and so on.
Mode	Global Configuration Mode
Default	priority - 32768

☞ The priority value can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

This priority value configuration is not supported in PVRST Mode.

Example

```
Your Product(config)#spanning-tree priority 4096
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `show spanning-tree root` - Displays the spanning tree root information.
- `show spanning-tree bridge` - Displays the spanning tree bridge information.
- `show spanning-tree - Summary, Blockedports, Pathcost, Redundancy` – Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `instance` - Creates an MST instance and maps it to VLANs.
- `show spanning-tree mst - CIST or specified mst Instance` Displays multiple spanning tree information for all MSTIs in the switch.
- `show spanning-tree mst - Port Specific Configuration` - Displays multiple spanning tree port specific information for the specified port.

16.11 spanning-tree auto-edge

Command Objective	This command enables automatic detection of Edge port parameter of an interface. The no form of this command disables automatic detection of Edge port parameter of an interface. The automatic detection of Edge port parameter is disabled, even if the spanning tree Mode is changed. Once automatic detection is enabled, the Edge port parameter is automatically detected and set. The port is set as edge port, if no BPDU is received on the port. The port is set as non-edge port, if any BPDU is received.

Syntax	`spanning-tree auto-edge`
	
	`no spanning-tree auto-edge`

Mode	Interface Configuration Mode (Physical Interface Mode)
Default	Automatic detection of Edge port parameter of an interface is enabled.
☞	The automatic detection of Edge port parameter can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.
Example	`Your Product(config-if)# spanning-tree auto-edge`
Related Command(s)	• `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch. • `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.

16.12 spanning-tree - Properties of an interface

Command Objective

This command configures the port related spanning tree information for all kinds of STPs. This can be applied for any port, in RSTP/MSTP Mode. This command creates port in STP when Automatic Port Create feature is disabled.

The no form of this command resets the port related spanning tree information to its default value. The port related spanning tree information is changed to its default value even if the spanning tree Mode is changed. This command also deletes port in STP when Automatic Port Create feature is disabled.

In STP module, whenever a port is mapped to any context, the corresponding port is created irrespective of whether STP is intended to be enabled on that interface. This leads To STP scaling issues and this problem is solved by having control at STP module on the port entry creation at STP module itself.

Syntax

```
spanning-tree [{cost <value(0-
200000000)>|disable|link- type{point-to-
point|shared}|portfast|port-priority<value(0-
240)>}]

no spanning-tree [{cost |disable|link-
type|portfast|port- priority}]
```

Parameter

Description

- `cost <value(0-200000000)>` - Configures the port's path cost value that contributes to the path cost of paths containing this particular port. The paths' path cost is used during calculation of shortest path to reach the root. The path cost represents the distance between the root port and designated port. This value ranges between 1 and 200000000. The configured path cost is used, even if the dynamic pathcost calculation feature or LAGG speed feature is enabled. This configuration is not supported for the spanning tree Mode pvrst.
- `disable` - Disables the spanning tree operation on the port. The port does not take part in the execution of spanning tree operation for preventing undesirable loops in the network.

- **link-type** - Configures the link status of the LAN segment attached to the port. The options available are:
  - **point-to-point** – The port is treated as if it is connected to a point-to-point link.
  - **shared** - The port is treated as if it is using a shared media connection.
- **portfast** - Configures the portfast feature in the port. This feature specifies that the port is connected to only one hosts and hence can rapidly transit to forwarding. This feature can cause temporary bridging loops, if hubs, concentrators, switches, bridges and so on are connected to this port. This feature takes effect only when the interface is shutdown.
- **port-priority <value(0-240)>** - Configures the priority value assigned to the port. This value is used during port role selection process. This value ranges between 0 and 240. This value should be set in steps of 16, that is, you can set the value as 0, 16, 32, 48, and so on. This configuration is not supported for the spanning tree Mode pvrst.

Mode Interface Configuration Mode (Physical Interface Mode)

Default

- cost - 200000 for all physical ports, 199999 for port channels
- disable - Spanning tree operation is enabled in the port.
- link-type - The port is considered to have a point-to-point link if:
  - It is an aggregator and all of its members can be aggregated.
  - The MAC entity is configured for full duplex operation, either manually or through auto negotiation process (that is, negotiation Mode is set as **Auto**)
  - Otherwise port is considered to have a shared media connection
- portfast - Portfast is disabled.
- port-priority - 128

☞ The port-related spanning tree information can be configured, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

This command executes without the optional parameters only if automatic port- create feature is disabled.

Example

```
Your Product(config-if)# spanning-tree cost 2200

Your Product(config-if)# spanning-tree link-type
point-to- point

Your Product(config-if)# spanning-tree portfast

Your Product(config-if)# spanning-tree port-priority
32

Your Product(config-if)# spanning-tree
```

Related Command(s)

- `automatic-port-create` – Enables or disables the Automatic Port Create feature.
- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree pathcost dynamic` - Enables dynamic pathcost calculation feature in the switch.
- `show spanning-tree - Summary, Blockedports, Pathcost, Redundancy` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.
- `show spanning-tree root` - Displays the spanning tree root information.
- `show spanning-tree mst - CIST or specified mst Instance` - Displays multiple spanning tree information for all MSTIs in the switch.
- `show spanning-tree mst - Port Specific Configuration` - Displays multiple spanning tree port specific information for the specified port.

- **`show spanning-tree vlan - Summary, Blockedports, Pathcost`** - Displays PVRST related information for the specified VLAN.

16.13 spanning-tree portfast - disable | trunk

Command Objective	This command configures the portfast Mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire. This command is a standardized implementation of the existing command; `spanning-tree - Properties of an interface.` It operates similar to the existing command. The spanning-tree portfast feature is currently not supported in the Global Configuration Mode.
Syntax	`spanning-tree portfast { disable | trunk}`
Parameter **Description**	• `disable` - Disables PortFast Mode\
Mode	Global Configuration Mode
Example	`Your Product(config)# spanning-tree portfast trunk`
Related Command(s)	• `spanning-tree Mode -pvrst` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch. • `show spanning-tree interface` - Displays the spanning tree port specific configuration.

16.14 spanning-tree portfast - bpdufilter default | bpduguarddefault | default

Command Objective	This command configures the portfast of the non-trunk ports as bpdufilter default or bpduguard default or default. This is used only for Trunk ports.
	This command is a standardized implementation of the existing command; `spanning-tree - Properties of an interface.` It operates similar to the existing command. The spanning-tree portfast feature is currently not supported in the Global Configuration Mode.
Syntax	`spanning-tree portfast {bpdufilter default	bpduguard default	default}`  `no spanning-tree portfast {bpdufilter default	bpduguard default	default}`

Parameter

Description

- `bpdufilter default` - Enables BPDU filtering on all PortFast ports.
- `bpduguard default` - Enables BPDU guard feature on all PortFast ports.
- `default` - Enables PortFast by default on all access ports.

Mode	Global Configuration Mode
Example	`Your Product(config)# spanning-tree portfast default`

Related Command(s)

- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.

- `show spanning-tree interface` - Displays the spanning tree port specific configuration.

16.15 spanning-tree restricted-role

Command Objective	This command enables the restricted role feature for a port. The restricted role feature blocks the port from being selected as a root port even if it has the best spanning tree priority vector. This port is selected as an alternate port after the root port is selected. This feature allows you to block switches external to a core region of the network from influencing the spanning tree active topology. The blocking of port from being selected as a root port can cause lack of spanning tree connectivity. The no form of this command disables the restricted role feature in the port. The restricted role feature is disabled, even if the spanning tree Mode is changed or port is set as L2GP.

Syntax	`spanning-tree restricted-rol`
	
	`no spanning-tree restricted-role`

Mode	Interface Configuration Mode (Physical Interface Mode)
Default	Restricted role feature is disabled in all ports.
☞	The restricted role feature can be configured, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown. This configuration is not supported in PVRST Mode.
Example	`Your Product(config-if)# spanning-tree restricted-role`

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree layer2-gateway-port` - Configures a port to operate as a L2GP.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.

16.16 spanning-tree restricted-tcn

Command Objective	This command enables the topology change guard / restricted TCN feature on a port. The restricted TCN feature blocks the port from propagating the received topology change notifications and topology changes to other ports. This feature allows you to block switches external to a core region of the network from causing address flushing in the region. The blocking of port can cause temporary loss of connectivity after changes in a spanning tree active topology as a result of persistent incorrectly learnt station location information. The no form of this command disables the topology change guard / restricted TCN feature on the port. The topology change guard / restricted TCN feature is disabled, even if the spanning tree Mode is changed or port is set as L2GP.

Syntax	`spanning-tree restricted-tcn`
	
	`no spanning-tree restricted-tcn`

Mode	Interface Configuration Mode (Physical Interface Mode)
Default	Topology change guard / restricted TCN feature is disabled in all ports..
☞	The topology change guard / restricted TCN feature can be configured, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown. This configuration is not supported in PVRST Mode.
Example	`Your Product(config-if)# spanning-tree restricted-tcn`

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree layer2-gateway-port` - Configures a port to operate as a L2GP.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.

16.17 spanning-tree layer2-gateway-port

Command Objective	This command configures a port to operate as a L2GP. L2GP operates similar to that of the normal port operation but pretends to continuously receive BPDUs when admin state of the port is Up. The no form of this command configures the port to operate as a normal port. The port operates as normal port, even if the spanning tree Mode is changed.

Syntax	`spanning-tree layer2-gateway-port`
	
	`no spanning-tree layer2-gateway-port`

Mode	Interface Configuration Mode (Physical Interface Mode)
Default	The port operates as a normal port.

☞

- The port can be configured as L2GP, only if the BPDU transmit status, restricted role feature and restricted TCN feature of the port are disabled.
- The PIP or CBP ports cannot be set as L2GP.
- Ports with SISP enabled interfaces cannot be set as L2GP.
- The port state of the L2GP is always set as discarding.
- The topology change guard / restricted TCN feature can be configured, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example	`Your Product(config-if)# spanning-tree layer2-gateway-port`

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree restricted-role` - Enables the restricted role feature for a port.
- `spanning-tree restricted-tcn` - Enables the topology change guard/ restricted TCN feature on a port.
- `spanning-tree bpdu-transmit` - Configures the BPDU transmission status of a port.
- `show spanning-tree - Summary, Blockedports, Pathcost, Redundancy` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree detail` – Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.
- `show spanning-tree – layer 2 gateway port` - Displays spanning tree information for all L2GPs enabled in the switch.
- `show spanning-tree mst - CIST or specified mst Instance` - Displays multiple spanning tree information for all MSTIs in the switch.
- `show spanning-tree mst - Port Specific Configuration` - Displays multiple spanning tree port specific information for the specified port.
- `show spanning-tree vlan - Summary, Blockedports, Pathcost` - Displays PVRST related information for the specified VLAN.
- `show spanning-tree vlan - interface` - Displays interface specific PVRST information for the specified VLAN.

16.18 spanning-tree bpdu-receive

Command Objective

This command configures the processing status of the BPDUs received in a port. BPDUs are used to carry bridge related information that is used during spanning tree operation.

The processing status is reset to its default value, once the spanning tree Mode is changed.

Syntax

```
spanning-tree bpdu-receive {enabled | disabled}
```

Parameter

Description

- `enabled` - Allows normal processing of BPDUs received on the port.
- `disabled` - Discards the BPDUs received on the port.

Mode

Interface configuration Mode (Physical Interface Mode)

Default

Enabled

The processing status of the received BPDUs can be configured, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example

```
Your Product(config-if)# spanning-tree bpdu-
receive disabled
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.

- **spanning-tree Mode** - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- **show spanning-tree detail** - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- **show spanning-tree active detail** - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- **show spanning-tree interface** - Displays the port related spanning tree information for the specified interface.

16.19 spanning-tree bpdu-transmit

Command Objective	This command configures the BPDU transmission status of a port. BPDUs are used to carry bridge related information that is used during spanning tree operation. The transmission status is reset to its default value, once the spanning tree Mode is changed.
Syntax	`spanning-tree bpdu-transmit {enabled | disabled}`
Parameter Description	• `enabled` - Allows the transmission of BPDUs from the port. • `disabled` - Blocks the transmission of BPDUs from the port.
Mode	Interface configuration Mode (Physical Interface Mode)
Default	enabled
☞	• BPDU transmission status cannot be enabled on the port that is configured as L2GP. • The BPDU transmission status can be configured, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.
Example	`Your Product(config-if)# spanning-tree bpdu-transmit enabled`
Related Command(s)	• `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.

- **spanning-tree Mode** - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- **spanning-tree layer2-gateway-port** - Configures a port to operate as a L2GP.
- **show spanning-tree detail** - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- **show spanning-tree active detail** - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- **show spanning-tree interface** - Displays the port related spanning tree information for the specified interface.

16.20 spanning-tree loop-guard

Command Objective	This command enables the loop guard feature in a port. This feature prevents the alternative or root ports from becoming designated ports due to failure in a unidirectional link. This feature is useful when the neighbor bridge is faulty, that is, the bridge cannot send BPDUs but continues to send data traffic. The no form of this command disables the loop guard feature in the port. The loop guard feature is disabled, even if the spanning tree Mode is changed.

Syntax	`spanning-tree loop-guard`
	
	`no spanning-tree loop-guard`

Mode	Interface Configuration Mode (Physical Interface Mode)
Package	Workgroup, Enterprise Metro_E and Metro
☞	The loop guard feature can be configured, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.
Example	`Your Product(config-if)# spanning-tree loop-guard`
Related Command(s)	• `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch. • `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch. • `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.

- `show spanning-tree active detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.

16.21 spanning-tree – Pseudoroot configuration

Command Objective

This command configures the pseudoroot related information for a port set as L2GP.

The information contains pseudoroot priority and pseudoroot MAC address for the port. This configuration is not utilized in PVRST Mode.

The no form of this command resets the pseudoroot related information to the currently available bridge related information.

Syntax

```
spanning-tree [mst <instance-id>] pseudoRootId
priority <value(0-61440)> mac-address <ucast_mac> no
spanning-tree [mst <instance-id(1-64)>] pseudoRootId
```

Parameter Description

- `mst <instance-id>/ mst <instance-id(1-64)>` - Configures the ID of MSTP instance already created in the switch. This value ranges between 1 and 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs. This option is applicable, only if the spanning tree Mode is set as mst.
- `priority <value(0-61440)>` - Configures the priority of the pseudoroot. Port configured as L2GP uses this value in generated BPDUs as the root identifier. This value ranges between 0 and 61440. The value should be set in steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288 and so on.
- `mac-address` - Configures the unicast MAC address of the pseudoroot. Port configured as L2GP uses this value as its address.

Mode

Interface configuration Mode (Physical Interface Mode)

Default

- priority - Priority value assigned to the switch.
- mac-address - MAC address assigned to the switch.

☞ The pseudoroot related information can be configured, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example

```
Your Product(config-if)# spanning-tree mst 1
pseudoRootId priority 8192 mac-address
00:00:12:34:45:55
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree interface` – Displays the port related spanning tree information for the specified interface.
- `show spanning-tree – layer 2 gateway port` - Displays spanning tree information for all L2GPs enabled in the switch.
- `instance` - Creates an MST instance and maps it to VLANs.
- `show spanning-tree mst - CIST or specified mst Instance` - Displays multiple spanning tree information for all MSTIs in the switch.
- `show spanning-tree mst - Port Specific Configuration` – Displays multiple spanning tree port specific information for the specified port.
- `show spanning-tree vlan - Summary, Blockedports, Pathcost` - Displays PVRST related information for the specified VLAN.
- `show spanning-tree vlan - interface` - Displays interface specific PVRST information for the specified VLAN.

16.22 debug spanning-tree

Command Objective

This command enables the tracing of the STP module as per the configured debug levels. The trace statements are generated for the configured trace levels.

This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command.

The no form of this command disables the tracing of the STP module as per the configured debug levels. The trace statements are not generated for the configured trace levels.

Syntax

```
debug spanning-tree { global | all | [errors]
[init-shut] [management] [memory] [bpdu] [events]
[timer] [port-info- state-machine] [port-recieve-
state-machine] [port-role- selection-state-
machine] [role-transition-state-machine] [state-
transition-state-machine] [protocol-migration-
state-machine] [topology-change-state-machine]
[port- transmit-state-machine] [bridge-detection-
state-machine] [pseudoInfo-state-machine]
[redundancy] [sem-variables] [switch
<context_name>]}
```

```
no debug spanning-tree {global | {all | errors |
init-shut | management | memory | bpdu |events |
timer | state-machine {port-info | port-receive |
port-role-selection | role-transition | state-
transition | protocol-migration | topology-change |
port-transmit | bridge-detection | pseudoInfo }
redundancy | sem-variables} [switch <context_name>]}
```

Parameter

Description

- `global` - Generates debug statements for global traces. This trace is used for providing status of STP task initialization, memory-pool creation and event-reception in STP task.

This parameter is specific to Multiple Instance.

- **all** - Generates debug statements for all kinds of traces.
- **errors** - Generates debug statements for all failure traces.
- **init-shut** - Generates debug statements for init and shutdown traces. This trace is generated on failed and successful initialization and shutting down of STP related module and memory.
- **management** - Generates debug statements for management traces. This trace is generated whenever you configure any of the STP features.
- **memory** - Generates debug statements for memory related traces. This trace is generated on failed and successful allocation of memory for STP process.
- **bpdu** - Generates debug statements for BPDU related traces. This trace is generated on failed and successful reception, transmission and processing of BPDUs.
- **events** - Generates debug statements for event handling traces. This trace is generated to denote events that are posted to STP configuration queue whenever you configure any of the STP features.
- **timer** - Generates debug statements for timer module traces. This trace is generated on failed and successful start, stop and restart of STP timers.
- **port-info-state-machine** - Generates debug statements for port information SEM.
- **port-recieve-state-machine** - Generates debug statements for port receive SEM.
- **port-role-selection-state-machine** - Generates debug statements for role selection SEM.
- **role-transition-state-machine** - Generates debug statements for role transition SEM.
- **state-transition-state-machine** - Generates debug statements for state transition SEM.
- **protocol-migration-state-machine** - Generates debug statements for protocol migration SEM.
- **topology-change-state-machine** - Generates debug statements for topology change SEM.
- **port-transmit-state-machine** - Generates debug statements for port transmit SEM.
- **bridge-detection-state-machine** - Generates debug statements for bridge detection SEM.
- **pseudoInfo-state-machine** - Generates debug statements for port receive pseudo information SEM.
- **state machine** - Generates debug statements to denote the event and state of the selected SEM. The options are:
  - **port-info** - Generates debug statements for port information SEM.
  - **port-receive** - Generates debug statements for port receive SEM.

- **port-role-selection** - Generates debug statements for role selection SEM.
- **role-transition** - Generates debug statements for role transition SEM.
- **state-transition** - Generates debug statements for state
- transition SEM.
- **protocol-migration** - Generates debug statements for protocol migration SEM.
- **topology-change** - Generates debug statements for topology change SEM.
- **port-transmit** - Generates debug statements for port transmit
- SEM.
- **bridge-detection** - Generates debug statements for bridge detection SEM.
- **pseudoInfo** - Generates debug statements for port receive pseudo information SEM.

- **redundancy** - Generates debug statements for redundancy code flow traces. This trace is generated in standby node STP while taking backup of configuration information from active node.
- **sem-variables** - Generates debug statements for state machine variable changes traces. This trace is generated on failed and successful creation and deletion of semaphore.
- **switch<context_name>** - Configures the tracing of the STP module for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode	Privileged EXEC Mode
Default	Tracing of the STP module is disabled

16.23 clear spanning-tree detected protocols

Command Objective	This command restarts the protocol migration process on all interfaces in the switch and forces renegotiation with the neighboring switches.
Syntax	`clear spanning-tree detected protocols [{interface <interface-type> <interface-id> | switch <context_name>}]`

Parameter Description	• `interface <interface-type> <interface-id>` - Restarts the protocol migration process on the specified interface. The details to be provided are:
	  • `<interface-type>` - Sets the type of interface. The interface can be:
	  ▪ qx-ethernet – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
	  ▪ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
	  ▪ extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
	  ▪ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
	  • `<interface-id>` - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface types port-channel.
	  • `switch <context_name>` - Restarts the protocol migration process for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode	Privileged EXEC Mode
Example	`Your Product# clear spanning-tree detected protocols interface gigabitethernet 0/1`

Related Command(s)

- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.

16.24 show spanning-tree - Summary, Blockedports, Pathcost, Redundancy

Command Objective	This command displays spanning tree related information available in the switch for the current STP enabled in the switch. The information contains priority, address and timer details for root and bridge, status of dynamic pathcost calculation feature, status of spanning tree function, STP compatibility version used, configured spanning tree Mode, bridge and port level spanning tree statistics information, and details of ports enabled in the switch. The port details contain port ID, port role, port state, port cost, port priority and link type.
Syntax	`show spanning-tree [{ summary | blockedports | pathcost method | redundancy }] [ switch <context_name>]`
Parameter Description	• `summary` - Displays the currently used STP, applied path cost method and port details such as port ID, port role, port state and port status. This option cannot be executed in the PVRST Mode. • `blockedports` - Displays the list of ports in blocked state and the total number of blocked ports. This option cannot be executed in the PVRST Mode. • `pathcost method` - Displays the port pathcost method configured for the switch. • `redundancy` - Displays the port role and port state, and dumps the STP port related information. • `switch <context_name>` - Displays the STP related information in the switch, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode

☞ This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example Single Instance:

```
Your Product# show spanning-tree

Root Id         Priority   32768
                Address    ac:1f:6b:f0:b2:91
                Cost       0
                Port       0
                This bridge is the root
                Max age 20 sec 0 cs, forward delay 15 sec 0 cs
                Hello Time 2 sec 0 cs
MST00
Spanning tree Protocol has been enabled
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id       Priority  32768
                Address  ac:1f:6b:f0:b2:91
                Max age is 20 sec 0 cs, forward delay is 15 sec 0 cs
                Hello Time is 2 sec 0 cs
                Dynamic Path Cost is Enabled
                Dynamic Path Cost Lag-Speed Change is Enabled
Name              Role         State        Cost     Prio    Type
----              ----         -----        ----     ----    ------
Ex0/1             Designated   Forwarding   2000     128     P2P
Ex0/3             Designated   Forwarding   2000     128     P2P
Ex0/5             Designated   Forwarding   2000     128     P2P
Ex0/9             Designated   Forwarding   2000     128     P2P
Ex0/21            Designated   Forwarding   2000     128     P2P
Ex0/57            Designated   Forwarding   2000     128     P2P
Ex0/61            Designated   Forwarding   2000     128     P2P
Ex0/62            Designated   Forwarding   2000     128     P2P

Your Product# show spanning-tree blockedports
```

```
Blocked Interfaces List:
Ex0/3,
The Number of Blocked Ports in the system is :1
Your Product# show spanning-tree pathcost method
Spanning Tree port pathcost method is Long
Your Product# show spanning-tree summary
Spanning tree enabled protocol is RSTP
Spanning Tree port pathcost method is Long
RSTP Port Roles and States
Port-Index  Port-Role    Port-State   Port-Status
----------  ---------    ----------   -----------
Ex0/1       Disabled     Discarding   Enabled
Ex0/2       Disabled     Discarding   Enabled
Ex0/3       Disabled     Discarding   Enabled
Ex0/4       Disabled     Discarding   Enabled
Ex0/5       Disabled     Discarding   Enabled
Ex0/6       Disabled     Discarding   Enabled
For RSTP
Your Product# show spanning-tree redundancy
Port Role/State for Instance 0 Port 1
======================
Port Role 3 Port State 5
Port Role/State for Instance 0 Port 2
======================
Port Role 1 Port State 2
Dumping Data On Port 1
------------------------
RootId 0:00:11:22:33:44:55
Designated BrId 0:00:11:22:33:44:55
Root path Cost 0
Length 0
```

```
Protocol Id 0

Port Id 8001

Message Age 0

Max Age 14

Hello Time 2

Fwd Delay Time 15

Dest Addr 00:00:00:00:00:00

Src Addr 00:00:00:00:00:00

Version Length 0

Version 2

BPDU Type 2

Flags e

Dumping Data On Port 2

------------------------
RootId 0:00:11:22:33:44:55

Designated BrId 0:00:11:22:33:44:55

Root path Cost 0

Length 0

Protocol Id 0

Port Id 8002

Message Age 0

Max Age 14

Hello Time 2

Fwd Delay Time 15

Dest Addr 00:00:00:00:00:00

Src Addr 00:00:00:00:00:00

Version Length 0

Version 2
```

```
BPDU Type 2

Flags e

Instance 0 Port 1

======================

Expected FdWile expiry time 0

Expected rcvdInfo exp Time 4654

Expected rrWhile exp Time 0

Expected rbWhile exp Time 0

Expected tcWhile exp Time 0

Instance 0 Port 1

TCN Var 1

STP Version 1

Proposing Flag 0

Info Is 4

Instance 0 Port 2

======================

Expected FdWile expiry time 0

Expected rcvdInfo exp Time 4656

Expected rrWhile exp Time 0

Expected rbWhile exp Time 0

Expected tcWhile exp Time 0

Instance 0 Port 2

TCN Var 1

STP Version 1

Proposing Flag 0

Info Is 4
```

Multiple Instance: For RSTP

```
Your Product# show spanning-tree

Switch default

We are the root of the Spanning Tree

Root Id    Priority   32768

           Address    00:05:02:03:04:01

           Cost   0

           Port   0

           Max Age 20 sec 0 cs, Forward Delay 15 sec
           0 cs

Bridge is executing the rstp compatible

Rapid Spanning Tree

Protocol

Bridge Id   Priority 32768

            Address 00:05:02:03:04:01

            Hello Time 1 sec 58 cs, Max Age 20 sec 0
            cs

            Forward Delay 15 sec 0 cs

            Dynamic Path Cost is Disabled

            Dynamic Path Cost Lag-Speed Change is
            Enabled

Name         Role       State      Cost   Prio  Type
----         ----       -----      ----   ----  ----
```

For MSTP

```
Your Product# show spanning-tree

Switch default

Root Id          Priority   32768

     Address     00:01:02:03:04:01

     Cost        0

     Port        0[0]
```

```
        This bridge is the root

        Max age 20 Sec 0 cs, forward delay 15 Sec 0 cs

        Hello Time is 2 sec 0 cs

   MST00

   Spanning tree Protocol Enabled.

   S-VLAN Component: MST00 is executing the mstp
   compatible Multiple Spanning Tree Protocol

   Bridge Id    Priority  32768

                Address  00:01:02:03:04:01

                Max age 20 Sec 0 cs, forward delay 15
            Sec 0 cs

   Name         Role       State      Cost   Prio  Type
   ----         ----       -----      ----   ----  ----
```

Your Product# show spanning-tree summary

```
Switch - default

Spanning Tree port pathcost method is
Long Spanning tree enabled protocol is
MSTP MST00 Port Roles and States

Port-Index  Port-Role    Port-State     Port-Status
----------  ---------    ----------     -----------

49          Disabled     Forwarding   Disabled

Switch - cust1

Spanning Tree port pathcost method is
Long Spanning tree enabled protocol is
MSTP MST00 Port Roles and States

Port-Index  Port-Role    Port-State     Port-Status
----------  ---------    ----------     -----------

1           Designated   Forwarding   Enabled

2           Root         Forwarding   Enabled

3           Designated   Forwarding   Enabled
```

```
4           Disabled     Discarding   Enabled

5           Disabled     Discarding   Enabled

6           Disabled     Discarding   Enabled

Switch - cust2

Spanning Tree port pathcost method is

Long Spanning tree enabled protocol is

MSTP MST00 Port Roles and States
```

Port- Index	Port-Role	Port-State	Port Status
7	Designated	Forwarding	Enabled
8	Root	Forwarding	Enabled
9	Alternate	Discarding	Enabled
10	Disabled	Discarding	Enabled

Related Command(s)

- **shutdown - physical/VLAN/port-channel/tunnel Interface** - Disables a physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface.
- **shutdown spanning-tree** - Shuts down spanning tree functionality in the switch.
- **spanning-tree** - Enables the spanning tree operation in the switch for the selected spanning tree Mode.
- **spanning-tree Mode** - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- **spanning-tree compatibility** - Sets the STP compatibility version in the switch for all ports.
- **spanning-tree timers** - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- **spanning-tree pathcost dynamic** - Enables dynamic pathcost calculation feature in the switch.
- **spanning-tree priority** - Configures the priority value that is assigned to the switch.

- **spanning-tree - Properties of an interface** - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- **spanning-tree layer2-gateway-port** - Configures a port to operate as a L2GP.
- **spanning-tree mst- Properties of an interface for MSTP** - Configures the port related spanning tree information for a specified MSTI.
- **spanning-tree mst hello-time** - Configures the hello time for an interface that is enabled.
- **spanning-tree vlan** - Configures spanning tree related information on a per VLAN basis.
- **spanning-tree vlan status** - Configures the status of PVRST on a port for the specified VLAN.
- **spanning-tree vlan port-priority** - Configures the priority of a port for the specified VLAN.
- **spanning-tree vlan cost** - Configures the cost of a port for the specified VLAN.

16.25 show spanning-tree detail

Command Objective	This command displays detailed spanning tree related information of the switch and all ports enabled in the switch. The information contains status of spanning tree operation, current selected spanning Mode, current spanning tree compatibility version, bridge and root priority, bridge and root addresses, port path cost, port priority, port timers, bridge and port level spanning tree statistics information, transmit hold-count value, link-type, and status of L2GP, loop guard, BPDU receive, BPDU transmit, restricted TCN, restricted role and portfast features.
Syntax	`show spanning-tree detail [ switch <context_name>]`
Parameter Description	• `switch <context_name>` - Displays detailed spanning tree related information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode
☞	This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.
Example	Single Instance

```
Your Product# show spanning-tree detail

Spanning tree Protocol Enabled.

Bridge is executing the rstp compatible Spanning Tree

Protocol
```

```
Bridge Identifier has priority 32768, Address

00:01:02:03:04:01

Configured Hello time 2 sec 0 cs, Max Age 20 sec

0 cs, Forward Delay 15 sec 0 cs

Dynamic Path Cost Disabled

We are the root of the spanning tree

Number of Topology Changes 0

Time since topology Change 0 seconds ago

Transmit Hold-Count 6

Root Times:Max Age 20 sec 0 cs   Forward Delay 15 sec 0
cs

Hello Time 2 sec 0 cs

Port 1 [Gi0/1] is Designated, Discarding

Port PathCost 200000, Port Priority 128, Port
Identifier

128.1

Designated Root has priority 32768, address

00:01:02:03:04:01

Designated Bridge has priority 32768, address

00:01:02:03:04:01

Designated Port Id is 128.1, Designated PathCost 0

No of Transitions to forwarding State :0

PortFast is disabled

Link Type is Shared

BPDUs : sent 3 , recieved 0

Timers: Hello - 1, Forward Delay - 14, Topology Change
- 0

Restricted Role is

disabled. Restricted TCN

is disabled. bpdu-

transmit enabled
```

```
bpdu-receive enabled
```

Multiple Instance:

```
Your Product# show spanning-tree detail switch default

Switch default

MST00 is executing the mstp compatible Multiple
Spanning Tree Protocol

Bridge Identifier has Priority 32768, Address

00:51:02:03:04:05

Configured  Max age 20 sec 0 cs, Forward delay 15 sec 0
cs

Configured Hello Time 2 sec 0 cs

Dynamic Path Cost Disabled

Flush Interval 0 centi-sec, Flush Invocations 1

Flush Indication threshold 0

We are root of the spanning tree

Current Root has priority 32768, address

00:51:02:03:04:05

cost of root path is 0

Number of Topology Changes 1, Time since topology
Change 82 seconds ago

Transmit Hold-Count 3

Root Times: Max age 20 sec 0 cs  Forward delay 15 sec 0
cs

Port 1 [Gi0/1] of MST00 is Designated, Forwarding

Gi0/1 is operating in the MSTP Mode

Port path cost  200000, Port priority  128,

Port Identifier  128.1. Port HelloTime  2 secs 0 cs,

Timers: Hello - 0, Forward Delay - 0, Topology Change
- 0

Designated root has priority 32768, address
```

```
00:51:02:03:04:05

Designated Bridge has priority 32768, address

00:51:02:03:04:05

Designated Port Id is 128.1, Designated pathcost is 0

Operational Forward delay 15 sec 0 cs, Max age 20 sec 0
cs

Number of Transitions to forwarding State: 1

PortFast is disabled

Link Type is Shared

BPDUs : sent 58, recieved 0

Restricted Role is disabled. Restricted TCN is
disabled.
```

Related Command(s)

- **shutdown - physical/VLAN/port-channel/tunnel Interface** - Disables a physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface.
- **shutdown spanning-tree** - Shuts down spanning tree functionality in the switch.
- **spanning-tree** - Enables the spanning tree operation in the switch for the selected spanning tree Mode.
- **spanning-tree Mode** - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- **spanning-tree compatibility** - Sets the STP compatibility version in the switch for all ports.
- **spanning-tree timers** - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- **spanning-tree transmit hold-count** - Sets the transmit hold-count value for the switch.
- **clear spanning-tree counters** - Deletes all bridge and port level spanning tree statistics information.
- **spanning-tree pathcost dynamic** - Enables dynamic pathcost calculation feature in the switch.
- **spanning-tree priority** - Configures the priority value that is assigned to the switch.

- **spanning-tree - Properties of an interface** - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- **spanning-tree restricted-role** - Enables the restricted role feature for a port.
- **spanning-tree restricted-tcn** - Enables the topology change guard / restricted TCN feature on a port.
- **spanning-tree layer2-gateway-port** - Configures a port to operate as a L2GP.
- **spanning-tree bpdu-receive** - Configures the processing status of the BPDUs received in a port.
- **spanning-tree bpdu-transmit** - Configures the BPDU transmission status of a port.
- **spanning-tree loop-guard** - Enables the loop guard feature in a port.
- **spanning-tree – Pseudoroot configuration** - Configures the pseudoroot related information for a port set as L2GP.
- **spanning-tree mst- Properties of an interface for MSTP** - Configures the port related spanning tree information for a specified MSTI.
- **spanning-tree mst hello-time** - Configures the hello time for an interface that is enabled.
- **spanning-tree vlan** - Configures spanning tree related information on a per VLAN basis.
- **spanning-tree vlan status** - Configures the status of PVRST on a port for the specified VLAN.
- **spanning-tree vlan port-priority** - Configures the priority of a port for the specified VLAN.
- **spanning-tree vlan cost** - Configures the cost of a port for the specified VLAN.
- **spanning-tree flush-interval** – Configures the flush interval timer value.
- **spanning-tree flush-indication-threshold** - Configures the flush indication threshold value for a specific instance.

16.26 show spanning-tree active

Command Objective	This command displays spanning tree related information available in the switch for the current STP enabled in the switch. The information contains priority, address and timer details for root and bridge, status of dynamic pathcost calculation feature, status of spanning tree function, STP compatibility version used, configured spanning tree Mode, bridge and port level spanning tree statistics information, and details of ports enabled in the switch. The port details contain port ID, port role, port state, port cost, port priority and link type.
Syntax	`show spanning-tree active [detail] [ switch <context_name>]`
Parameter Description	• `detail` – Displays detailed spanning tree related information of the switch and all ports enabled in the switch. The information contains status of spanning tree operation, current selected spanning Mode, current spanning tree compatibility version, bridge and root priority, bridge and root addresses, port path cost, port priority, port timers, bridge and port level spanning tree statistics information, transmit hold-count value, link-type, and status of L2GP, loop guard, BPDU receive, BPDU transmit, restricted TCN, restricted role and portfast features • `switch <context_name>` - Displays spanning tree related information available in the switch, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode
☞	This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The

type of spanning tree Mode should be set, if the functionality is already shutdown.

Example

Single Instance:

```
Your Product# show spanning-tree active
Root Id     Priority   32768
Address    00:01:02:03:04:01
Cost     200000
Port       1 [Gi0/1]
Max age 20 sec 0 cs, forward delay 15 sec 0 cs
Hello Time 2 sec 0 cs
MST00
Spanning tree Protocol has been enabled
MST00 is executing the mstp compatible Multiple Spanning
Tree Protocol
Bridge Id   Priority  32768
Address  00:02:02:03:04:01
Max age 20 sec 0 cs, forward delay 15 sec 0 cs
Hello Time 2 sec 0 cs
Dynamic Path Cost is Disabled
Name       Role       State      Cost       Prio  Type
----       ----       -----      ----       ----  ------
Gi0/1      Root       Forwarding 200000     128   SharedLan
```

Multiple Instance:

```
Your Product# show spanning-tree active switch default
Switch default
Root Id     Priority   32768
Address    00:51:02:03:04:05
Cost       0
```

```
Port        0 [0]
This bridge is the root
-Max age 20 sec 0 cs, forward delay 15 sec 0 cs
Hello Time 2 sec 0 cs
MST00
MST00 is executing the mstp compatible Multiple Spanning
Tree Protocol
Bridge Id   Priority  32768
Address  00:51:02:03:04:05
Max age 20 sec 0 cs, forward delay 15 sec 0 cs
Hello Time 2 sec 0 cs
Name  Role        State       Cost        Prio        Type
----  ----        -----       ----        ----        ------
Gi0/1 Designated  Forwarding  200000      128         SharedLan
```

Related Command(s)

- **shutdown - physical/VLAN/port-channel/tunnel Interface** - Disables a physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface.
- **shutdown spanning-tree** - Shuts down spanning tree functionality in the switch.
- **spanning-tree** - Enables the spanning tree operation in the switch for the selected spanning tree Mode.
- **spanning-tree Mode** - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- **spanning-tree compatibility** - Sets the STP compatibility version in the switch for all ports.
- **spanning-tree timers** - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- **spanning-tree transmit hold-count** - Sets the transmit hold-count value for the switch.
- **clear spanning-tree counters** - Deletes all bridge and port level spanning tree statistics information.

- **spanning-tree pathcost dynamic** - Enables dynamic pathcost calculation feature in the switch.
- **spanning-tree priority** - Configures the priority value that is assigned to the switch.
- **spanning-tree – Properties of an interface** - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- **spanning-tree restricted-role** - Enables the restricted role feature for a port.
- **spanning-tree restricted-tcn** - Enables the topology change guard / restricted TCN feature on a port.
- **spanning-tree layer2-gateway-port** - Configures a port to operate as a L2GP.
- **spanning-tree bpdu-receive** - Configures the processing status of the BPDUs received in a port.
- **spanning-tree bpdu-transmit** - Configures the BPDU transmission status of a port.
- **spanning-tree loop-guard** - Enables the loop guard feature in a port.
- **spanning-tree – Pseudoroot configuration** - Configures the pseudoroot related information for a port set as L2GP.
- **spanning-tree mst- Properties of an interface for MSTP** - Configures the port related spanning tree information for a specified MSTI.
- **spanning-tree vlan** - Configures spanning tree related information on a per VLAN basis.
- **spanning-tree vlan status** - Configures the status of PVRST on a port for the specified VLAN.
- **spanning-tree vlan port-priority** - Configures the priority of a port for the specified VLAN.
- **spanning-tree vlan cost** - Configures the cost of a port for the specified VLAN.

16.27 show spanning-tree interface

Command Objective

This command displays the port related spanning tree information for the specified interface.

The information contains port ID, port role, port state, port cost, port priority and link type. The generic command cannot be executed without any option in the PVRST Mode.

Syntax

```
show spanning-tree interface <interface-type>
<interface- id> [{ cost | priority | portfast |
rootcost | restricted- role | restricted-tcn | state
| stats | detail }]
```

Parameter

Description

- `<interface-type>` - Displays the port related spanning tree information for the specified type of interface. The interface can be:

–qx-ethernet – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.

–gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

–extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.

–port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.

- `<interface-id>` - Displays the port related spanning tree information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For Example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. For Example: 1 represents port-channel ID.
- `cost` - Displays the cost of the port or instances assigned to that port. This option cannot be executed in the PVRST Mode.
- `priority` - Displays the priority of the port or instances assigned to that port. This option cannot be executed in the PVRST Mode.

- **portfast** - Displays the status of the portfast feature for the port or instances assigned to that port.
- **rootcost** - Displays the root cost of the port or instances assigned to that port. The root cost defines the pathcost to reach the root bridge. This option cannot be executed in the PVRST Mode.
- **restricted-role** - Displays the status of the restricted role feature for the port. This option cannot be executed in the PVRST Mode.
- **restricted-tcn** - Displays the status of the restricted TCN feature for the port. This option cannot be executed in the PVRST Mode.
- **state** - Displays the state of the port. This option cannot be executed in the PVRST Mode.
- **stats** - Displays the port level spanning tree statistics information. This option cannot be executed in the PVRST Mode.
- **detail** - Displays detailed spanning tree related information for the port. The information contains current selected spanning Mode, bridge and root priority, bridge and root addresses, port path cost, port priority, port timers, bridge and port level spanning tree statistics information, link-type, and status of L2GP, loop guard, BPDU receive, BPDU transmit, restricted TCN, restricted role and portfast features. This option cannot be executed in the PVRST Mode.

Mode Privileged EXEC Mode

This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode

should be set, if the functionality is already shutdown.

Example

Single Instance

```
Your Product# show spanning-tree interface
gigabitethernet 0/1

Instance     Role         State        Cost         Prio   Type
--------     ----         -----        ----         ----   ----
```

MST00 Root Forwarding 200000 128.1 SharedLan

Your Product# show spanning-tree interface gigabitethernet 0/1 cost

Port cost is 200000

Your Product# show spanning-tree interface gigabitethernet

0/1 priority

Port Priority is 128

Your Product# show spanning-tree interface gigabitethernet

0/1 portfast

PortFast is disabled

Your Product# show spanning-tree interface gigabitethernet

0/1 rootcost

Root Cost is 200000

Your Product# show spanning-tree interface gigabitethernet

0/1 stateISS

Forwarding

Your Product# show spanning-tree interface gigabitethernet

0/1 stats

Statistics for Port Gi0/1

Number of Transitions to forwarding State: 1

Number of RSTP BPDU Count received: 1692

Number of Config BPDU Count received: 9

Number of TCN BPDU Count received: 0

Number of RSTP BPDU Count Transmitted: 735

Number of Config BPDU Count Transmitted: 11

Number of TCN BPDU Count Transmitted: 0

Number of Invalid BPDU Count Transmitted: 0

Port Protocol Migration Count: 1

Your Product# show spanning-tree interface gigabitethernet

0/1 detail

Port 1 [Gi0/1] is Designated, Forwarding

Port PathCost 200000, Port Priority 128, Port Identifier

128.1

Designated Root has priority 32768, address

00:01:02:03:04:01

Designated Bridge has priority 32768, address

00:01:02:03:04:01

Designated Port Id is 128.1, Designated PathCost 0

No of Transitions to forwarding State :2

PortFast is enabled

Link Type is Shared

BPDUs : sent 1780 , recieved 254

Timers: Hello - 0, Forward Delay - 0, Topology Change - 0

Restricted Role is disabled.

Restricted TCN is disabled.

bpdu-transmit enabled

bpdu-receive enabled

Your Product# show spanning-tree interface fast 0/1 restricted-role

Restricted Role is Disabled

Your Product# show spanning-tree interface fast 0/1 restricted-tcn

Restricted TCN is Disabled

Multiple Instance:

Your Product# show spanning-tree interface gigabitethernet 0/1

```
Switch      Default
Role        State       Cost        Prio        Type
----        -----       ----        ----        ----
Root        Forwarding  200000      128         SharedLan
```

Your Product# show spanning-tree interface gigabitethernet 0/1 cost

```
Port cost is 200000
Switch - default
```

Your Product# show spanning-tree interface gigabitethernet 0/1 priority

```
Switch – default
Port Priority is 128
```

Your Product# show spanning-tree interface gigabitethernet 0/1 portfast Switch – default
PortFast is disabled

Your Product# show spanning-tree interface gigabitethernet 0/1 rootcost

```
Switch – default
Root Cost is 200000
```

Your Product# show spanning-tree interface gigabitethernet 0/1 state

```
Switch – default
Forwarding
```

Your Product# show spanning-tree interface gigabitethernet 0/1 stats

```
Switch – default
Statistics for Port Gi0/1
Number of Transitions to forwarding State: 1
```

Number of RSTP BPDU Count received: 1692

Number of Config BPDU Count received: 9

Number of TCN BPDU Count received: 0

Number of RSTP BPDU Count Transmitted: 735

Number of Config BPDU Count Transmitted: 11

Number of TCN BPDU Count Transmitted: 0

Number of Invalid BPDU Count Transmitted: 0

Port Protocol Migration Count: 1

Your Product# show spanning-tree interface gigabitethernet 0/1 detail

Switch – default

Port 1 [Gi0/1] is Root , Forwarding

Port PathCost 200000, Port Priority 128, Port Identifier

128.1

Designated Root has priority 8192, address

00:01:02:03:04:21

Designated Bridge has priority 8192, address

00:01:02:03:04:21

Designated Port Id is 128.1, Designated PathCost 0

No of Transitions to forwarding State :1

PortFast is disabled

Link Type is Shared

BPDUs : sent 735 , recieved 1729

Your Product# show spanning-tree interface fast 0/1 restricted-role

Switch – default

Restricted Role is Disabled

Your Product# show spanning-tree interface fast 0/1 restricted-tcn

```
Switch - default

Restricted TCN is Disabled
```

Related Command(s)

- **shutdown spanning-tree** - Shuts down spanning tree functionality in the switch.
- **spanning-tree** - Enables the spanning tree operation in the switch for the selected spanning tree Mode.
- **spanning-tree Mode** - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- **spanning-tree timers** - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- **clear spanning-tree counters** - Deletes all bridge and port level spanning tree statistics information.
- **spanning-tree priority** - Configures the priority value that is assigned to the switch
- **spanning-tree - Properties of an interface** - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- **spanning-tree restricted-role** - Enables the restricted role feature for a port.
- **spanning-tree restricted-tcn** - Enables the topology change guard / restricted TCN feature on a port.
- **spanning-tree layer2-gateway-port** - Configures a port to operate as a L2GP
- **spanning-tree bpdu-receive** - Configures the processing status of the BPDUs received in a port.
- **spanning-tree bpdu-transmit** - Configures the BPDU transmission status of a port.
- **spanning-tree loop-guard** - Enables the loop guard feature in a port.
- **spanning-tree - Pseudoroot configuration** - Configures the pseudoroot related information for a port set as L2GP.
- **clear spanning-tree detected protocols** - Restarts the protocol migration process on all interfaces in the switch and forces renegotiation with the neighboring switches.
- **spanning-tree mst- Properties of an interface for MSTP** - Configures the port related spanning tree information for a specified MSTI.

- **`spanning-tree mst hello-time`** - Configures the hello time for an interface that is enabled.
- **`spanning-tree bpduguard`** - Configures the status of BPDU guard feature in an interface.

16.28 show spanning-tree root

Command Objective	This command displays the spanning tree root information. The information contains root ID, root path cost, maximum age time, forward delay time and root port, for the RSTP. The information also contains the instance ID for MSTP.
Syntax	`show spanning-tree root [{ address | cost | forward-time | id | max-age | port | priority | detail }] [ switch <context_name>]`
Parameter	
Description	• `address` - Displays the MAC address of the root bridge. • `cost` - Displays the cost of the root bridge. • `forward-time` - Displays the forward delay time of the root bridge. • `id` - Displays the ID of the root bridge. • `max-age` - Displays the maximum age time of the root bridge. • `port` - Displays the ID of the root port. • `priority` - Displays the priority of the root bridge. • `detail` - Displays the root priority, root address, root cost, root port, forward delay time and maximum age time. • `switch <context_name>` - Displays spanning tree root information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode
☞	This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown. This configuration is not supported in PVRST Mode.

Example

Single Instance:

```
                    Your Product# show spanning-tree root
Root ID                    RootCost   MaxAge     FwdDly     RootPort
-------                    --------   ------     ------     --------
80:00:00:01:02:03:04:11    0          20 sec     0 cs 15 sec 0 cs  0
 Your Product# show spanning-tree root  address
 Root Bridge Address is 00:01:02:03:04:11
 Your Product# show spanning-tree root cost
 Root Cost is 0
 Your Product# show spanning-tree root forward-time
 Forward delay is 15 sec 0 cs
 Your Product# show spanning-tree root id
 Root Bridge Id is 80:00:00:01:02:03:04:11
 Your Product# show spanning-tree root max-age
 Root MaxAge is 20 secs 0 cs
 Your Product# show spanning-tree root port
 Root Port is 0
 Your Product# show spanning-tree root  priority
 Root Priority is 32768
 Your Product# show spanning-tree root detail
 We are the root of the Spanning Tree
 Root Id     Priority   32768
             Address    00:01:02:03:04:11
             Cost       0
             Port       0
             Max Age 20 sec 0 cs, Forward Delay 15 sec 0 cs
```

Multiple Instance:

```
Your Product# show spanning-tree root

Switch - default

Instance    Root   ID     RootCost      MaxAge FwdDly RootPort

--------  -------        --------      ------ ------ --------

MST00       80:00:00:01:02:03:04:01 0         20 sec 0 cs 15 sec 0 cs 0

Switch - cust1 Instance  Root ID RootCost MaxAge FwdDly RootPort

----  -------               --------    ------   ------   --------

MST00 00:00:00:01:02:03:04:04 200000  20 sec  0 cs  15 sec 0 cs    Gi0/2
```

Related Command(s)

- **spanning-tree Mode** - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- **spanning-tree timers** - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- **spanning-tree priority** - Configures the priority value that is assigned to the switch.
- **spanning-tree - Properties of an interface** - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- **spanning-tree mst hello-time** - Configures the hello time for an interface that is enabled.

16.29 show spanning-tree bridge

Command Objective

This command displays the spanning tree bridge information. The information contains bridge ID, hello time, maximum age time, forward delay time and protocol enabled, for the RSTP. The information also contains the instance ID for MSTP.

Syntax

```
show spanning-tree bridge [{ address | forward-time |
hello-time | id | max-age | protocol | priority |
detail}] [ switch <context_name>]
```

Parameter

Description

- `address` - Displays the MAC address of the bridge.
- `forward-time` - Displays the forward delay time of the bridge.
- `hello-time` - Displays the hello time of the bridge.
- `id` - Displays the ID of the bridge.
- `max-age` - Displays the maximum age time of the bridge.
- `protocol` - Displays the protocol currently enabled in the bridge.
- `priority` - Displays the priority of the bridge.
- `detail` - Displays the priority, address, maximum age time and forward delay time for the bridge.
- `switch` - Displays spanning tree bridge information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode

Privileged EXEC Mode

This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

This configuration is not supported in PVRST Mode.

Example

Single Instance:

```
Your Product# show spanning-tree  bridge forward-time

Bridge Forward delay is  15 sec

Your Product# show spanning-tree bridge

Bridge ID           HelloTime   MaxAge    FwdDly   Protocol

---------           ---------  ------     ------  ------

80:00:00:01:02:03:04:21  2 s 0 cs  20  s 0 cs 15   s 0 cs    rstp

Your Product# show spanning-tree bridge  hello-time

Bridge Hello Time is 2 sec 0 cs

Your Product# show spanning-tree bridge  id

Bridge ID is 80:00:00:01:02:03:04:21

Your Product# show spanning-tree bridge  max-age

Bridge Max Age is 20 sec 0 cs

Your Product# show spanning-tree bridge protocol

Bridge Protocol Running is RSTP

Your Product# show spanning-tree bridge priority

Bridge Priority is 32768

Your Product# show spanning-tree bridge  detail

Bridge Id     Priority 32768

              Address  00:05:02:03:04:01

              Max age is 20 sec 0 cs, forward delay is
              15 sec 0 cs
```

Multiple Instance:

```
Your Product# show spanning-tree bridge

MST Instance Bridge ID                 MaxAge FwdDly Protocol

------------ ---------                  ------ ------ --------

MST00        32788 ac:1f:6b:f0:b2:91    20      15      mstp

MST10

Bridge Id     Priority 32778

              Address  ac:1f:6b:f0:b2:91
```

```
                Max age is 20 sec 0 cs, forward delay is
15 sec 0 cs

Protocolmstp

MST20

Bridge Id       Priority 32788

                Address  ac:1f:6b:f0:b2:91

                Max age is 20 sec 0 cs, forward delay is
15 sec 0 cs
```

Your Product# show spanning-tree bridge address

```
Switch - default

MST00      00:01:02:03:04:01

Switch - cust1
```

Related Command(s)

- **shutdown spanning-tree** - Shuts down spanning tree functionality in the switch.
- **spanning-tree** - Enables the spanning tree operation in the switch for the selected spanning tree Mode.
- **spanning-tree Mode** - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- **spanning-tree timers** - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- **spanning-tree priority** - Configures the priority value that is assigned to the switch.
- **spanning-tree mst hello-time** - Configures the hello time for an interface that is enabled.

16.30 show spanning-tree – layer 2 gateway port

Command Objective	This command displays spanning tree information for all L2GPs enabled in the switch. The information contains pseudoroot priority, pseudo root MAC address and state of the L2GP.
Syntax	`show spanning-tree [interface <interface-type> <interface- id>] layer2-gateway-port [switch <context_name>]`
Parameter Description	• `<interface-type>` - Displays L2GP related spanning tree information for the specified type of interface. The interface can be: ○ `qx-ethernet` – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links. ○ `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. ○ `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. ○ `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together. • `<interface-id>` - Displays L2GP related spanning tree information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For Example: 0/1 represents that the slot number is 0 andport number is only port-channel ID is provided, for interface type port-channel. For example: 1 represents port-channel ID. • `switch <context_name>` - Displays L2GP related spanning tree information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode

☞ This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example

```
Your Product# show spanning-tree interface
gigabitethernet 0/1 layer2-gateway-port switch default

Switch default

Port Gi0/1

PseudoRootId

Instance      Priority         MacAddress          State

----------  ----------   -------------------  ----------
MST00        4096        00:00:11:22:33:44   Forwarding
MST01        8192        00:00:12:34:45:55   Forwarding
MST02        4096        00:00:12:34:45:5a   Forwarding
```

Related Command(s)

- **shutdown - physical/VLAN/port-channel/tunnel Interface** - Disables a physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface.
- **shutdown spanning-tree** - Shuts down spanning tree functionality in the switch.
- **spanning-tree Mode** - Sets the typeof spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- **spanning-tree layer2-gateway-port** – Configures a port to operate as a L2GP.
- **spanning-tree – Pseudoroot configuration** - Configures the pseudoroot related information for a port set as L2GP.

16.31 show customer spanning-tree

Command Objective	This command displays the detailed customer spanning tree information.
Syntax	`show customer spanning-tree [cep interface <interface- type> <interface-number>] [{ detail [active] | active [detail] }]`
Parameter Description	• `cep interface<interface-type>` - Displays the Customer Edge Port interface details. The details to be provided are: • `<interface-type>` - Displays the customer spanning tree related information for the CEP type of interface. The interface can be: • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. • <interface-number> - Displays the customer spanning tree related information for the CEP interface number. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. For Example: 0/1 represents that the slot number is 0 and port number is 1. Only internal-lan and port- channel ID is provided, for interface types internal-lan and port- channel. For Example: 1 represents internal-lan and port-channel ID. • `detail` - Displays in detail about the port and bridge. This includes designated Bridge details, designated port details, timer values, root bridge and so on. • `active` - Displays the Bridge and details of the active (active ports are those ports that are participating in the spanning-tree) ports.

Mode	Privileged EXEC Mode

☞ The port must be configured as CEP. This feature is not available on some SMIS switch models.

Example

Single Instance:

```
Your Product# show customer spanning-tree cep
interface fast 0/1

Port [Gi0/1]

We are the root of the Spanning Tree

Root Id       Priority   65535

               Address    00:01:02:03:04:01

              Cost     0

              Root Ports

               Hello Time 2 Sec 0 cs, Max Age 20 Sec 0 cs,
               Forward Delay 15 Sec 0 cs

Customer Spanning Tree Enabled Protocol RSTP
Bridge Id     Priority 65535

               Address 00:01:02:03:04:01

               Hello Time 2 Sec 0 cs, Max Age 20 Sec 0 cs,
               Forward Delay 15 Sec 0 cs

Name      Role      State        Cost     Prio    Type

----       ----     -----        ----     ----    ------

PEP-Service: 2 Designated  Forwarding  128    32   SharedLan

CEP-Gi0/1     Designated  Forwarding  200000 32   SharedLan

Your Product# show customer spanning-tree

Port [Gi0/1]

We are the root of the Spanning Tree

Root Id         Priority   65535
```

```
                    Address     00:01:02:03:04:01
                     Cost       0
                     Root Ports
Hello Time 2 Sec, Max Age 0 Sec, Forward
Delay 0 Sec
Customer Spanning Tree Enabled Protocol RSTP
Bridge Id      Priority 65535
                  Address 00:01:02:03:04:01
                  Hello Time 2 Sec 0 cs, Max Age 20 Sec 0 cs,
                  Forward Delay 15 Sec 0 cs
Name       Role     State         Cost      Prio    Type
----       ----     -----         ----      ----    ------
PEP-Service: 2   Designated    Forwarding 128 32 SharedLan
CEP-Gi0/1   Designated    Forwarding   200000   32 SharedLan
```

Multiple Instance:

```
Your Product# show customer spanning tree
Switch default
Port [Gi0/1]
We are the root of the Spanning Tree
Root Id        Priority    65535
                  Address     00:01:02:03:04:01
                   Cost       0
                   Root Ports
                  Hello Time 2 Sec 0 cs, Max Age 20 Sec 0 cs,
                  Forward Delay 15 Sec 0 cs
Customer Spanning Tree Enabled Protocol RSTP
Bridge Id       Priority 65535
                    Address 00:01:02:03:04:01
                   Hello Time 2 Sec 0 cs, Max Age 20 Sec 0 cs,
                   Forward Delay 15 Sec 0 cs
Name       Role          State         Cost      Prio    Type
```

```
----      ----          -----         ----      ----    ------ PEP-
Service: 2   Designated  Forwarding  128    32 SharedLan CEP-Gi0/1
Designated  Forwarding 200000 32 SharedLan
```

Your Product# show customer spanning-tree cep interface fastethernet 0/1

```
Switch default

Port [Gi0/1]

We are the root of the Spanning Tree

Root Id       Priority   65535

               Address    00:01:02:03:04:01

                Cost       0

                Root Ports

               Hello Time 2 Sec 0 cs, Max Age 20 Sec 0 cs,
               Forward Delay 15 Sec 0 cs

Customer Spanning Tree Enabled Protocol RSTP
Bridge Id     Priority 65535

               Address 00:01:02:03:04:01

               Hello Time 2 Sec 0 cs, Max Age 20 Sec 0 cs,

               Forward Delay 15 Sec 0 cs

               Name        Role    State      Cost    Prio   Type

                ----      ----    -----     ----    ----  ----
```

Related Command(s)

- **show customer spanning-tree** – Displays the detailed customer spanning information

---

16.32 spanning-tree forwarddelay optimization alternate-role

Command Objective	This command enables or disables the optimization for spanning-tree related protocol during transition from alternate to designated port role. When role translation takes place from alternate to designated, the value with which forward-delay timer started is controlled by executing this command.
Syntax	`spanning-tree forwarddelay optimization alternate-role {enabled | disabled}`
Parameter Description	• `enabled` - Enables optimization for spanning-tree related protocol in alternate port role transition. • `disabled` - Disables the optimization for spanning-tree related protocol in alternate port role transition.
Mode	Global Configuration Mode
☞	This command executes only if the RSTP is enabled.
Default	enabled
Example	`Your Product(config)# spanning-tree forwarddelay optimization alternate-role enabled`
Related Command(s)	

- **`spanning-tree mode`** - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch. The current selected type of spanning tree is enabled and the existing spanning tree type is disabled in the switch.

17 MSTP

Aricent MSTP is a portable implementation of the IEEE 802.1s standard. It is used to configure spanning tree on per VLAN basis or multiple VLANs per spanning tree. It allows you to build several MST over VLAN trunks, and group or associate VLANs to spanning tree instances, so the topology of one instance is independent of the other instance. It provides multiple forwarding paths for data traffic and enables load balancing. It improves the overall network fault tolerance, as failure in one instance does not affect the other instances.

This section describes all the commands for MSTP Configurations. The list of commands for the configuration of MSTP is as follows:

- **spanning-tree mst max-hops**
- **spanning-tree mst configuration**
- **spanning-tree mst max-instance**
- **spanning-tree mst root**
- **spanning-tree mst forward-time**
- **spanning-tree mst max-age**
- **name**
- **revision**
- **instance**
- **spanning-tree mst- Properties of an interface for MSTP**
- **spanning-tree mst hello-time**
- **show spanning-tree mst - CIST or specified mst Instance**
- **show spanning-tree mst configuration**
- **show spanning-tree mst - Port Specific Configuration**
- **spanning-tree flush-interval**
- **spanning-tree flush-indication-threshold**

17.1 spanning-tree mst max-hops

Command Objective	This command configures the maximum number of hops permitted in the MSTP. This value ranges between 6 and 40. The number of hops represents the maximum number of switches that a packet can cross before it is dropped. The switch uses this value to avoid infinite looping of the packets, if it is elected as the root switch in the topology. The root switch always transmits a BPDU with the maximum hop count value. The receiving switch decrements the value by one and propagates the BPDU with modified hop count value. The BPDU is discarded and the information held is aged out, when the count reaches 0. The no form of this command resets the maximum number of hops to its default value.
Syntax	`spanning-tree mst max-hops <value(6-40)>`
Mode	Global Configuration Mode
Default	2
☞	This command can be executed successfully, only if the spanning tree functionality is started in the switch. The type of spanning tree Mode should be set as mst.
Example	`Your Product(config)#spanning-tree mst max-hops 10`

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `show spanning-tree mst - CIST or specified mst Instance` - Displays multiple spanning tree information for all MSTIs in the switch.

- **`show spanning-tree mst - Port Specific Configuration`** - Displays multiple spanning tree port specific information for the specified port.

17.2 spanning-tree mst configuration

Command Objective	This command enters into MSTP configuration Mode, where instance specific and MST region configuration can be done.
Syntax	`spanning-tree mst configuration`
Mode	Global Configuration Mode
☞	This command can be executed successfully, only if the spanning tree functionality is started and enabled in the switch. The type of spanning tree Mode should be set as mst.
Example	`Your Product(config)#spanning-tree mst configuration`
Related Command(s)	• `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch. • `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.

17.3 spanning-tree mst max-instance

Command Objective	This command configures the maximum number of active MSTIs that can be created. This value ranges between 1 and 64. This configuration allows you to limit the number of spanning tree instances to be allowed in the switch. This does not count the special MSTID such as PTETID, used to identify the VIDs which are used by ESPs. The no form of this command resets maximum MSTP instance value to its default value.

Syntax	`spanning-tree mst max-instance <short(1-64)>`
	
	`no spanning-tree mst max-instance`

Mode	Global Configuration Mode
Default	64
☞	This command can be executed successfully, only if the spanning tree functionality is started and enabled in the switch. The type of spanning tree Mode should be set as mst.
Example	`Your Product(config)# spanning-tree mst max-instance 40`
Related Command(s)	• `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch. • `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch. • `instance` - Creates an MST instance and maps it to VLANs.

17.4 spanning-tree mst root

Command Objective	This command enables BPDU (Bridge Protocol Data Unit) transmission and reception on the interface. This command is a standardized implementation of the existing command; `spanning-tree priority`. It operates similar to the existing command . The no form of the command disables BPDU transmission and reception on the interface.

Syntax	`spanning-tree mst {instance-id <instance-id(1-64)>} root {primary | secondary}`
	
	`no spanning-tree mst {instance-id <instance-id(1-64)>} root`

Parameter Description	• `instance-id <instance-id(1-64)>` - Configures the ID of MSTP instance already created in the switch. This value ranges between 1 and 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs. This option is applicable, only if the spanning tree Mode is set as mst. • `primary` - Sets high enough priority (low value) for the switch so that the switch can be made as the bridge root of the spanning-tree instance. The priority value is set as 24576. • `secondary` - Sets the switch as a secondary root, if the primary root fails. The priority value is set as 28672.
Mode	Global Configuration Mode
☞	This command executes only if • instance is created • spanning tree Mode is set as mst.

Example

```
Your Product(config)# spanning-tree mst instance-
id 1 root secondary
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree mst configuration` – Enters into MSTP configuration Mode, where instance specific and MST region configuration can be done.
- `instance` - Creates an MST instance and maps it to VLANs.
- `show spanning-tree detail` - Displays detailed spanning tree information
- `show spanning-tree active` - Displays spanning tree information of active ports

17.5 spanning-tree mst forward-time

Command Objective	This command configures the forward timer of the spanning tree and the no form of the command sets the forward timer to the default value. The forward timer controls the speed at which a port changes its spanning tree state from Blocking state to Forwarding state. The timer value ranges between 4 and 30 seconds. This command is currently not supported. The values configured for the spanning tree forward timers should satisfy the following conditions: 2* (forward-time - 1) >= max-age, and max-age >= 2 * (hello-time +1)
Syntax	`spanning-tree mst forward-time <seconds(4-30)>`
Mode	Global Configuration Mode
Default	`no spanning-tree mst forward-time` • forward-time - 15 secs
Example	**`Your Product(config)# spanning-tree mst forward-time 15`** SMIS(config)# spanning-tree mst forward-time 15 SMIS(config)# end SMIS# show spanning-tree bridge forward-time MST00 15 sec 0 cs
Related Command(s)	• `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch. • `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch information of the switch and all ports enabled in the switch.

- **show spanning-tree active** - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- **show spanning-tree interface detail** - Displays detailed spanning tree related information for the specified port.
- **show spanning-tree root** - Displays the spanning tree root information.
- **show spanning-tree bridge** - Displays the spanning tree bridge information.
- **show spanning-tree mst - CIST or specified mst Instance** - Displays multiple spanning tree information for all MSTIs in the switch.
- **show spanning-tree mst - Port Specific Configuration** - Displays multiple spanning tree port specific information for the specified port.

17.6 spanning-tree mst max-age

Command Objective	This command configures the max-age timer of the spanning tree. The max- age timer denotes the time (in seconds) after which the spanning tree protocol information learnt from the network on any port will be discarded. The timer value ranges between 6 and 40 seconds. The no form of the command sets the max-age timer to the default value Max-age timer can be configured in centi seconds through SNMP The values configured for the spanning tree forward timers should satisfy the following conditions: 2* (forward-time - 1) >= max-age, and max-age >= 2 * (hello-time +1) This command is a standardized implementation of the existing command; `spanning-tree timers`. It operates similar to the existing command.

Syntax	`spanning-tree mst max-age <seconds(6-40)>`
	
	`no spanning-tree mst max-age`

Mode	Global Configuration Mode
Default	• max-age - 20 secs

- The STP forward timers can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.
- This spanning tree timer's configuration is not supported in PVRST Mode.

Example

```
Your Product(config)# spanning-tree mst max-age 7
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `show spanning-tree - Summary, Blockedports, Pathcost, redundancy` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree interface detail` - Displays detailed spanning tree related information for the specified port.
- `show spanning-tree root` - Displays the spanning tree root information.
- `show spanning-tree bridge` - Displays the spanning tree bridge information.
- `show spanning-tree mst - CIST or specified mst Instance` - Displays multiple spanning tree information for all MSTIs in the switch.
- `show spanning-tree mst - Port Specific Configuration` - Displays multiple spanning tree port specific information for the specified port.

17.7 name

Command Objective	This command configures the name for the MST region. The name is unique and used to identify the specific MST region. Each MST region contains multiple spanning tree instances and runs special instance of spanning tree known as IST to disseminate STP topology information for other STP instances. The no form of this command resets the name to its default value.

Syntax	`name <string(32)>`
	
	`no name`

Default	Same as that of the base MAC address of the switch.
Example	`Your Product(config-mst)#name regionone`
Related Command(s)	• `show spanning-tree mst configuration` – Displays multiple spanning tree instance related information.

17.8 revision

Command Objective	This command configures the revision number for the MST region. This value ranges between 0 and 65535. The no form of this command resets the revision number to its default value.
Syntax	`revision <value(0-65535)>`
Mode	MSTP Configuration Mode
Default	0
Example	`Your Product(config-mst)#revision 100`

Related Command(s)

- `show spanning-tree mst configuration` – Displays multiple spanning tree instance related information.

17.9 Instance

Command Objective	This command creates an MST instance and maps it to VLANs. The no form of this command deletes the instance / unmaps specific VLANs from the MST instance.
Syntax	`instance <instance-id(1-64|4094)> vlan <vlan-range>`
Parameter	
Description	• `<instance-id(1-64|4094)>` - Configures the ID of MSTP instance to be created / deleted and mapped with / unmapped from VLAN. This value ranges between 1 to 64. The special value 4094 can be used in the switch that supports PBB-TE. Except vlan instance mapping, other commands for stp configurations will not be applicable in this Mode.This special value represents PTETID that identifies VID used by ESPs. • `vlan <vlan-range>` - Configures a VLAN ID or list of VLAN IDs that should be mapped with / unmapped from the specified MST instance. This value is a string whose maximum size is 9. For Example, the value is provided as 4000-4010 to represent the list of VLANs IDs from 4000 to 4010.
Mode	MSTP configuration Mode
Default	Instance 0 is created and mapped with all VLANs (1-4094).
Example	`Your Product(config-mst)#instance 2 vlan 2`
Related Command(s)	• `spanning-tree priority` - Configures the priority value that is assigned to the switch.

- **spanning-tree – Pseudoroot configuration** - Configures the pseudoroot related information for a port set as L2GP.
- **spanning-tree mst max-instance** - Configures the maximum number of active MSTIs that can be created.
- **spanning-tree mst- Properties of an interface for MSTP** - Configures the port related spanning tree information for a specified MSTI.
- **show spanning-tree mst - CIST or specified mst Instance** Displays multiple spanning tree information for all MSTIs in the switch.
- **show spanning-tree mst configuration** - Displays multiple spanning tree instance related information.
- **show spanning-tree mst - Port Specific Configuration** - Displays multiple spanning tree port specific information for the specified port

17.10 spanning-tree mst- Properties of an interface for MSTP

Command Objective	This command configures the port related spanning tree information for a specified MSTI in a port. The no form of this command resets the spanning tree information of a port to its default value.

Syntax

```
spanning-tree mst <instance-id(1-64)> { cost
<value(1-200000000)>| port-priority <value(0-240)> |
disable }

no spanning-tree mst <instance-id(1-
64)>{cost|port- priority | disable}
```

Parameter

Description

- `<instance-id(1-64)>` - Configures the ID of MSTP instance already created in the switch.This value ranges between 1 to 64.
- `cost<value(1-200000000)>` - Configures the port's path cost value that contributes to the path cost of paths containing this particular port. The paths' path cost is used during calculation of shortest path to reach the root. The path cost represents the distance between the root port and designated port. This value ranges between 1 and 200000000. The configured path cost is used, even if the dynamic pathcost calculation feature or LAGG speed feature is enabled.
- `port-priority<value(0-240)>` - Configures the priority value assigned to the port. This value is used during port role selection process. This value ranges between 0 and 240. This value should be set in steps of 16, that is, you can set the value as 0, 16, 32, 48, and so on. The MSTP puts the interface with lowest number in forwarding state and blocks all other interfaces, if all interfaces have the same priority value.
- `disable` - Disables the spanning tree operation on the port. The port does not take part in the execution of spanning tree operation for preventing undesirable loops in the network.

Mode	Interface Configuration Mode (Physical Interface Mode)

Default

- cost - 200000 for all physical ports; 199999 for port channels
- port-priority - 128
- disable - Spanning tree operation is enabled in the port.

This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set as mst

Example

```
Your Product(config-if)#spanning-tree mst 2 cost 4000

Your Product(config-if)#spanning-tree mst 1 port-priority32

Your Product(config-if)#spanning-tree mst 2 disable
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree pathcost dynamic` - Enables dynamic pathcost calculation feature in the switch.
- `instance` - Creates an MST instance and maps it to VLANs.
- `show spanning-tree - Summary, Blockedports, Pathcost,` redundancy - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.

- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.
- `show spanning-tree mst - CIST or specified mst Instance` Displays multiple spanning tree information for all MSTIs in the switch.

17.11 spanning-tree mst hello-time

Command Objective	This command configures the spanning tree hello time. The no form of this command resets the hello time to its default value. The hello time represents the time interval (in seconds) between two successive configuration BPDUs generated by the switch on the port. This value is either 1 or 2 seconds. This value is applied to all active MSTIs. Hello Time can be configured in centi seconds through SNMP

Syntax	`spanning-tree mst hello-time<value(1-2)>`
	
	`no spanning-tree mst hello-time`

Mode	Global Configuration Mode, Interface Configuration Mode (Physical Interface Mode)
Default	2 seconds
☞	This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set as mst.

Example	`Your Product(config-if)#spanning-tree mst hello-time 1`
	
	`Your Product(config)#spanning-tree mst hello-time 1`

Related Command(s)	• `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.

- **spanning-tree Mode** - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- **show spanning-tree - Summary, Blockedports, Pathcost, redundancy** - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- **show spanning-tree detail** - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- **show spanning-tree interface** - Displays the port related spanning tree information for the specified interface.
- **show spanning-tree root** - Displays the spanning tree root information.
- **show spanning-tree bridge** - Displays the spanning tree bridge information.
- **show spanning-tree mst - Port Specific Configuration** - Displays multiple spanning tree port specific information for the specified port.

17.12 show spanning-tree mst - CIST or specified mst Instance

Command Objective

This command displays multiple spanning tree information for all MSTIs in the switch.

The information contains MSTI ID, VLAN IDs mapped to the instance, bridge address and priority, root address and priority, IST root address, priority and path cost, forward delay, maximum age, maximum hop count, and port details of interfaces enabled in the switch. The port details contain interface ID, port role, port state, port cost, port priority and port link type.

Syntax

```
show spanning-tree mst [<instance-id(1-64|4094)>]
[detail] [ switch <context_name>]
```

Parameter

Description

- `<instance-id(1-64|4094)>` - Displays the multiple spanning tree information for the specified MSTI. This value ranges between 1 to 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs.
- `detail` - Displays the detailed multiple spanning tree information for the MSTI. This information contains MSTI ID, VLAN IDs mapped to the instance, bridge address and priority, root address and priority, IST root address, priority and path cost, forward delay, maximum age, maximum hop count, and BPDUs sent and received in the port.
- `switch<context_name>` - Displays multiple spanning tree bridge information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode

Privileged EXEC Mode

☞

This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set as mst.

Example **Single Instance:**

```
Your Product# show spanning-tree mst 1

## MST01

Vlans mapped:    2

Bridge     Address 00:01:02:03:04:11     Priority 32768

Root       Address 00:01:02:03:04:11     Priority 32768

Root       this switch for MST01

Interface Role   Sts    Cost   Prio.Nbr

--------- ----   ---    ----   --------

Gi0/1  Master   Forwarding   200000    128.1   SharedLan

Your Product# show spanning-tree mst 1 detail

 ## MST01

Vlans mapped:    2

Bridge     Address 00:01:02:03:04:11     Priority 32768

Root       Address 00:01:02:03:04:11     Priority 32768

Root       this switch for MST01

Gi0/1 of MST01 is Master    , Forwarding

Port info   port id 128.1     priority 128   cost 200000

Designated root   address 00:01:02:03:04:11     priority

32768 cost 0

Designated bridge address 00:01:02:03:04:11     priority

32768 port id 128.1
```

Multiple Instance:

```
Your Product# show spanning-tree mst 1

Switch - default

## MST01

Vlans mapped:    2

Bridge     Address 00:01:02:03:04:11     Priority 32768

Root       Address 00:01:02:03:04:11     Priority 32768

Root       this switch for MST01

Interface Role         Sts    Cost   Prio.  Nbr    Type
```

```
--------- ----          ---    ----   ------ ----

Gi0/1           Master Forwarding   200000 128.1 SharedLan
```

Related Command(s)

- **shutdown spanning-tree** - Shuts down spanning tree functionality in the switch.
- **spanning-tree** - Enables the spanning tree operation in the switch for the selected spanning tree Mode.
- **spanning-tree Mode** - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- **spanning-tree timers** - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- **clear spanning-tree counters** - Deletes all bridge and port level spanning tree statistics information.
- **spanning-tree priority** - Configures the priority value that is assigned to the switch.
- **spanning-tree - Properties of an interface** - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- **spanning-tree layer2-gateway-port** - Configures a port to operate as a L2GP.
- **spanning-tree – Pseudoroot configuration** - Configures the pseudoroot related information for a port set as L2GP.
- **spanning-tree mst max-hops** - Configures the maximum number of hops permitted in the MST.
- **instance** - Creates an MST instance and maps it to VLANs.
- **spanning-tree mst- Properties of an interface for MSTP** - Configures the port related spanning tree information for a specified MSTI.
- **shutdown - physical/VLAN/port-channel/tunnel Interface** - Disables a physical interface / VLAN interface / port-channel interface / tunnel interface.

17.13 show spanning-tree mst configuration

Command Objective

This command displays multiple spanning tree instance related information.

This information contains the MST region name, MST region revision, and a list containing MSTI IDs and VLAN IDs mapped to the corresponding MSTI.

Syntax

```
show spanning-tree mst configuration [ switch
```

Parameter

Description

- `switch <context_name>` - Displays multiple spanning tree instance related information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode

Privileged EXEC Mode

This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set as mst.

Example

Single Instance:

```
Your Product# show spanning-tree mst configuration

Name              [00:02:02:03:04:01]
Revision          0

Instance    Vlans mapped
--------    ----------------------------------------

0           1,3-1024,1025-2048,2049-3072, 3073-4094
1           2
```

```
-------------------------------------------------------
```

Multiple Instance:

```
Your Product# show spanning-tree mst configuration

Switch - default

Name       [00:01:02:03:04:01]

Revision   0

Instance   Vlans mapped

--------   ---------------------------------------

0          1-1024,1025-2048,2049-3072,3073-4094

-------------------------------------------------------

Switch - cust1

Name           [00:01:02:03:04:02] Revision        0

Instance       Vlans mapped

--------       ---------------------------------------
```

Related Command(s)

- **shutdown spanning-tree** - Shuts down spanning tree functionality in the switch.
- **spanning-tree Mode** - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- **name** - Configures the name for the MST region.
- **revision** - Configures the revision number for the MST region.
- **instance** - Creates an MST instance and maps it to VLANs.

17.14 show spanning-tree mst - Port Specific Configuration

Command Objective

This command displays multiple spanning tree port specific information for the specified port. This information contains interface ID, edge port status, port link type, port hello time, BPDUs sent and received on the port, and instance related details. The instance details contain MSTI ID, MSTI role, MSTI status, MSTI cost and MSTI priority.

Syntax

```
show spanning-tree mst [<instance-id(1-64|4094)>]
interface <interface-type><interface-id> [{ stats |
hello-time | detail }]
```

Parameter

Description

- `<instance-id(1-64|4094)>` - Displays the multiple spanning tree port specific information for the specified MSTI. This value ranges between 1 to 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs.
- `<interface-type>` - Displays the multiple spanning tree port specific information for the specified type of interface. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Displays the multiple spanning tree port specific information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For Example: 0/1 represents that the slotnumber is 0 and port number is 1. Only port-channel ID isprovided, for interface type port-channel. For Example: 1 represents port-channel ID.
- `stats` - Displays the number of BPDUs sent and received for the MSTIs assigned to the specified interface.

- **hello-time** - Displays the hello time of the MSTIs assigned to the specified interface.
- **detail** - Displays detailed multiple spanning tree port specific information for the specified interface. The information contains port priority, port cost, root address, priority and cost, IST address, priority and cost, bridge address, priority and cost, forward delay, maximum age, maximum hop count, and BPDUs sent and received.

Mode Privileged EXEC Mode

☞ This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set as mst.

Example

```
Your Product# show spanning-tree mst 1 interface
gigabitethernet 0/1

Switch default

Gi0/1 of MST00 is Disabled  , Discarding

Edge port: no

Link type: Shared

Port Hello Timer: 2 sec 0 cs

Bpdus sent 0 , Received 0

Instance  Role         Sts          Cost     Prio.Nbr

--------  ----         ---          ----     --------

0         Disabled     Discarding   200000   128.1

Your Product# show spanning-tree mst 1 interface
gigabitethernet 0/1 stats

MST01     Bpdus sent 2, Received 0

Your Product# show spanning-tree mst 1 interface
gigabitethernet 0/1 hello-time

MST01     2 secs 0 cs

Your Product# show spanning-tree mst 1 interface
gigabitethernet 0/1 detail
```

```
Gi0/1 of MST01 is Master    , Forwarding
Port info     port id 128.1       priority 128    cost
200000
Designated root  address 00:01:02:03:04:11     priority
32768 cost 0
Designated bridge address 00:01:02:03:04:11     priority
32768 port id 128.1
```

Related Command(s)

- **shutdown spanning-tree** - Shuts down spanning tree functionality in the switch.
- **spanning-tree Mode** - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- **spanning-tree timers** - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- **clear spanning-tree counters** - Deletes all bridge and port level spanning tree statistics information.
- **spanning-tree priority** - Configures the priority value that is assigned to the switch.
- **spanning-tree - Properties of an interface** - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- **spanning-tree layer2-gateway-port** – Configures a port to operate as a L2GP.
- **spanning-tree – Pseudoroot configuration** - Configures the pseudoroot related information for a port set as L2GP.
- **spanning-tree mst max-hops** - Configures the maximum number of hops permitted in the MST.
- **instance** - Creates an MST instance and maps it to VLANs.
- **spanning-tree mst hello-time** - Configures the hello time for an interface that is enabled.

17.15 spanning-tree flush-interval

Command Objective	This command configures the flush interval timer value (in centi-seconds), which controls the number of flush indications invoked from spanning-tree module per instance basis. This value ranges between 0 and 500 centi-seconds. If the flush interval timer is set to zero, port and instance-based flushing occurs (default functionality). If it is set to non-zero, instance-based flushing occurs (dependent on the flush-indication-threshold value). The no form of the command resets the flush-interval timer to the default value.
Syntax	`spanning-tree flush-interval <centi-seconds (0-500)>`
Mode	Global Configuration Mode
Default	flush-interval - 0 centi-secs
☞	This command executes only if the spanning tree Mode is set as mst.
Example	`Your Product(config)# spanning-tree flush-interval 20`

Related Command(s)

- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree flush-indication-threshold` – Sets the spanning tree flush indication threshold for a specific instance.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.

17.16 spanning-tree flush-indication-threshold

Command Objective	This command configures the flush indication threshold value for a specific instance. This indicates the number of flush indications to go before the flush- interval timer method triggers. This value ranges between 0 and 65535. When flush indication threshold is default value and flush interval is non- default value, instance-based flushing occurs during the first flush indication trigger. When the flush indication threshold value is non-default(x) and flush- interval value is non-default, port & instance-based flushing is triggered until the threshold(x) is reached. Once the threshold is reached, instance-based flushing is triggered & timer starts. The no form of the command sets the flush indication threshold of the specific instance to the default value.

Syntax	`spanning-tree [mst <instance-id>] flush-indication- threshold <value (0-65535)>`
	
	`no spanning-tree flush-indication-threshold`

Mode	Global Configuration Mode
Default	flush-indication-threshold - 0
☞	This command executes only if • the spanning tree Mode is set as mst. • the instance is created
Example	`Your Product(config)# spanning-tree flush-indication- threshold 2`

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree flush-interval` − Sets the spanning-tree flush interval timer value.
- `instance` - Creates an MST instance and maps it to VLANs.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.

18 LLDP

LLDP (Link Layer Discovery Protocol) supports a set of attributes that it uses to discover the neighbor devices. These attributes contain type, length, and value descriptions and are referred to as TLVs. LLDP supported devices can use TLVs to receive and send information to their neighbors.

The switch supports these mandatory basic management TLVs.

- Port description TLV
- System name TLV
- System description
- System capabilities TLV
- Management address TLV
- Port VLAN ID TLV ((IEEE 802.1 organizationally specific TLVs)
- MAC/PHY configuration/status TLV(IEEE 802.3 organizationally specific TLVs)

SMIS LLDP is a software implementation of the Link Layer Discovery Protocol (LLDP). It provides complete management capabilities using SNMP and CLI.

SMIS LLDP conforms to IEEE 802.1AB-2005 standard. The LLDP allows systems on an Ethernet LAN to advertise their key capabilities and also to learn about the key capabilities of other systems on the same Ethernet LAN. This, in turn, promotes a unified network management view of the LAN topology and connectivity to aid network administration and trouble-shooting.

SMIS LLDP provides the following features:

- Provides full conformance to the 802.1AB specification.
- Supports all mandatory TLVs (Chassis ID, Port ID and Time To Live).
- Supports optional TLVs - Port description, System name, System description, System capabilities and Management address.
- Supports organizationally specific optional TLVs - Port VLAN ID, Port and protocol VLAN ID, VLAN name, MAC or PHY configuration or status, Link Aggregation and Maximum frame size.
- Provides a generic set of APIs for easy integration into different platforms.
- Supports the basic MIB, as well as, the extension MIBs in Appendix F and Appendix G, defined in the 802.1AB specification and a proprietary MIB for management.
- Provides support for configuration and management by providing generic APIs usable from different management schemes like SNMP, CLI.
- Provides support for notifications through Traps.

- Conforms to Flexible Software Architecture for Portability (FSAP2), thus ensuring portable code, which uses flexible buffer and timer management libraries.

The list of CLI commands for the configuration of LLDP is as follows:

- `shutdown lldp`
- `set lldp`
- `lldp transmit-interval`
- `lldp holdtime-multiplier`
- `lldp reinitialization-delay`
- `lldp tx-delay`
- `lldp notification-interval`
- `lldp chassis-id-subtype`
- `clear lldp counters`
- `clear lldp table`
- `lldp transmit / receive`
- `lldp notification`
- `lldp tlv-select basic-tlv`
- `lldp port-id-subtype`
- `lldp tlv-select dot1tlv`
- `lldp tlv-select dot3tlv`
- `debug lldp`
- `show lldp`
- `show lldp interface`
- `show lldp neighbors`
- `show lldp traffic`
- `show lldp local`
- `show lldp errors`
- `show lldp statistics`
- `lldp dest-mac`
- `set lldp version`
- `lldp txCreditMax`
- `lldp MessageFastTx`
- `lldp txFastInit`
- `show lldp peer`

18.1 shutdown lldp

Command Objective	This command shuts down all the ports in the LLDP and releases all the allocated memory. The no form of the command enables all the ports by allocating the required resources in the LLDP

Syntax	`shutdown lldp`
	
	`no shutdown lldp`

Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro and Metro_E
☞	LLDP cannot be started in the switch, if the base bridge Mode is configured as transparent bridging.
Example	`Your Product(config)# shutdown lldp`

Related Command(s)

- `base bridge-Mode` - Configures the base Mode (either 802.1d transparent bridge Mode or 802.1q vlan aware bridge Mode) in which the VLAN feature should operate on the switch.
- `set lldp` - Transmits or receives LLDP frames from the server to the LLDP module
- `lldp transmit / receive` - Transmits or receives LLDP frames from the one of the ports of the server to the LLDP module.
- `lldp tlv-select basic-tlv` - Enables the basic settings while transmitting the LLDP frames on a given port.
- `lldp tlv-select dot1tlv` – Configures dot1 TLV while transmitting the LLDP frames to the particular port

- **lldp tlv-select dot3tlv** - Configures dot3 TLV while transmitting the LLDP frames to the particular port
- **lldp transmit-interval** - Sets the transmission time interval in which the server sends the LLDP frames to the LLDP module.
- **lldp holdtime-multiplier** - Sets the holdtime-multiplier value, which is the amount of time, the server should hold the LLDP.
- **lldp reinitialization-delay** - Sets the reinitialization delay time which is the minimum time an LLDP port will wait before reinitializing LLDP transmission.
- **lldp tx-delay** - Sets the transmit delay which is the minimum amount of delay between successive LLDP PDUs.
- **lldp notification** - Controls the transmission of LLDP notifications.
- **lldp notification-interval** - Sets the notification interval which is the minimum interval to generate a notification-event about a change in local system.
- **lldp chassis-id-subtype** - Configures an ID for LLDP chassis subtype which is a unique address of any module.
- **lldp port-id-subtype** - Configures an ID for LLDP port subtype
- **clear lldp counters** - Clears the inbuilt counter which has the total count of LLDP frames transmitted/received.
- **clear lldp table** - Clears all the LLDP information about the neighbors.
- **debug lldp** - Specifies debug level for LLDP module.
- **show lldp** - Displays the LLDP global configuration details to initialize on an interface.
- **show lldp interface** - Displays the information about interfaces where LLDP is enabled.
- **show lldp neighbors** - Displays information about neighbors on an interface or all interfaces.
- **show lldp traffic** - Displays LLDP counters on all interfaces or on a specific interface
- **show lldp local** - Displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces.
- **show lldp errors** - Displays the information about the errors such as memory allocation failures, queue overflows and table overflow.
- **show lldp statistics** - Displays the LLDP remote table statistics information.
- **lldp dest-mac** - Configures destination mac-address to be used by the LLDP agent for transmission on this port.
- **set lldp version** - Enables the lldp version to be used on the ports.

- **lldp txtCreditMax** - Configures the maximum number of consecutive LLDPDUs that can be transmitted any time.
- **lldp MessageFastTx** - Configures the interval at which LLDP frames are transmitted on behalf of this LLDP agent during fast transmission period.
- **lldp txFastInit** - Configures the initial value used to initialize the txFast variable which determines the number of transmissions that are made in fast transmission mode.

18.2 set lldp

Command Objective	This command transmits or receives LLDP frames from the server to the LLDP module.
Syntax	`set lldp {enable | disable}`
Parameter Description	• `enable` - Transmits/receives the LLDP packets between LLDP module and the server. • `disable` - Does not transmit/receive the LLDP packets between LLDP module and the server.
Mode	Global Configuration Mode
Default	Disable
☞	This command executes only if lldp is started.
Example	`Your Product(config)# set lldp enable`
Related Command(s)	• `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory. • `show lldp` – Displays LLDP global configuration details. • `show lldp interface` – Displays the information about interfaces where LLDP is enabled . • `show lldp neighbors` – Displays information about the neighbors on an interface or all interfaces. • `show lldp traffic` – Displays LLDP counters on all interfaces or on a specific interface

- **show lldp errors** – Displays the information about the errors such as memory allocation failures, queue overflows and table overflow.
- **show lldp statistics** – Displays the LLDP remote table statistics information.

18.3 lldp transmit-interval

Command Objective	This command sets the transmission interval in which the server sends the LLDP frames to the LLDP module. The value ranges between 5 and 32768 seconds. The no form of the command sets the transmission interval to the default value
Syntax	`lldp transmit-interval <seconds(5-32768)>`
Mode	Global Configuration Mode
Default	30 seconds
☞	This command executes only if lldp is started
Example	`Your Product(config)# lldp transmit-interval 50`
Related Command(s)	• `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory. • `show lldp` – Displays LLDP global configuration details.

18.4 lldp holdtime-multiplier

Command Objective

This command sets the holdtime-multiplier value, which is the amount of time, the server should hold the LLDP. The value ranges between 2 and 10 seconds.

The no form of the command sets the multiplier to the default value.

TLV (Time to Live) A value that tells the receiving agent, how long the information contained in the TLV Value field is valid.

TTL = message transmission interval * hold time multiplier.

For Example, if the value of LLDP transmission interval is 30, and the value of the LLDP hold multiplier is 4, then the value 120 is encoded in the TTL field in the LLDP header.

Syntax

```
lldp holdtime-multiplier <value(2-10)>

no lldp holdtime-multiplier
```

Mode

Global Configuration Mode

Default

4

This command executes only if lldp is started

Example

```
Your Product(config)# lldp holdtime-multiplier 5
```

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `show lldp` – Displays LLDP global configuration details.
- `lldp tx-delay` – Sets transmit delay which is the minimum amount of delay between successive LLDP frame transmissions.

18.5 lldp reinitialization-delay

Command Objective	This command sets the reinitialization delay time which is the minimum time an LLDP port will wait before reinitializing LLDP transmission. The value ranges between 1 and 10 seconds. The no form of the command sets the reinitialization delay time to the default value.

Syntax	`lldp reinitialization-delay <seconds(1-10)>`
	
	`no lldp reinitialization-delay`

Mode	Global Configuration Mode
Default	2 seconds ☞ This command executes only if lldp is started
Example	`Your Product(config)# lldp reinitialization-delay 4`
Related Command(s)	• `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory. • `show lldp` – Displays LLDP global configuration details.

18.6 lldp tx-delay

Command Objective	This command sets the transmit delay which is the minimum amount of delay between successive LLDP frame transmissions. The value ranges between 1 and 8192 seconds. The no form of the command sets the transmit delay to the default value. TxDelay should be less than or equal to (0.25 * Message Tx Interval)
Syntax	`lldp tx-delay <seconds(1-8192)>`
Mode	Global Configuration Mode
Default	2 seconds This command executes only if lldp is started
Example	`Your Product(config)# lldp tx-delay 120`

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `show lldp` - Displays LLDP global configuration details.
- `lldp holdtime-multiplier` – Sets the holdtime-multiplier value, which is the amount of time, the server should hold the LLDP.

18.7 lldp notification-interval

Command Objective

This command sets the time interval in which the local system generates a notification-event. In the specific interval, generating more than one notification-event is not possible. The value ranges between 5 and 3600 seconds.

The no form of the command sets the notification interval to the default value.

Syntax

```
lldp notification-interval <seconds(5-3600)>
```

Mode

Global Configuration Mode

Default

5 seconds

☞ This command executes only if lldp is started

Example

```
Your Product(config)# lldp notification-interval 150
```

Related Command(s)

- `show lldp` – Displays LLDP global configuration details.
- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.

18.8 lldp chassis-id-subtype

Command Objective

This command configures an ID for LLDP chassis subtype which is a unique address of any module.

Chassis id value can be set only for the chassis-component and local system subtypes. For all other subtypes, it takes the value from the system automatically.

Syntax

```
lldp chassis-id-subtype { chassis-comp <string(255)>
| if- alias | port-comp <string(255)> | mac-addr |
nw-addr | if- name | local <string(255)> }
```

Parameter Description

- `chassis-comp <string(255)>` - Represents a chassis identifier based on the value of entPhysicalAlias object for a chassis component.
- `if-alias` - Represents a chassis identifier based on the value of ifAlias for an interface on the containing chassis.
- `port-comp <string(255)>` - Represents a chassis identifier based on the value of entPhysicalAlias object for a port or backplane within the chassis.
- `mac-addr` - Represents a chassis identifier based on the value of a unicast source address, of a port on the chassis.
- `nw-addr` - Represents a chassis identifier based on a network address, associated with a particular chassis. The encoded address is actually composed of two fields. The first field is a single octet, representing the IANA AddressFamilyNumbers value for the specific address type, and the second field is the network address value.
- `if-name` - Represents a chassis identifier based on the value of ifName object for an interface on the containing chassis.
- `local <string(255)>` - Represents a chassis identifier based on a locally defined value."

Mode

Global Configuration Mode

This command executes only if lldp is started

Default mac-addr

Example

```
Your Product(config)# lldp chassis-id-subtype chassis-comp Aricentswitch

Your Product(config)# lldp chassis-id-subtype if-alias
```

Related Command(s)

- `show lldp` – Displays LLDP global configuration details.
- `show lldp local` – Displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces.
- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.

18.9 clear lldp counters

Command Objective

This command clears the inbuilt counter which has the total count of LLDP frames that are transmitted/ received.

This command does not clear the global statistics.

Syntax

```
clear lldp counters
```

Mode

Global Configuration Mode

This command executes only if lldp is started

Example

```
Your Product(config)# clear lldp counters
```

Related Command(s)

- `show lldp traffic` – Displays the LLDP counters on all interfaces or on a specific interface
- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.

18.10 clear lldp table

Command Objective	This command clears all the LLDP information about the neighbors.
Syntax	`clear lldp table`
Mode	Global Configuration Mode
☞	This command executes only if lldp is started
Example	`Your Product(config)# clear lldp table`

Related Command(s)

- `show lldp neighbors` – Displays information about the neighbors on an interface or all interfaces.
- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.

18.11 lldp transmit / receive

Command Objective

This command transmits or receives LLDP frames from the one of the ports of the server to the LLDP module.

The no form of the command resets LLDP admin status on an interface.

Syntax

```
lldp {transmit | receive} [mac-address <mac_addr>]

no lldp {transmit | receive} [mac-address <mac_addr>]
```

Parameter Description

- `transmit` - Enables transmission of LLDPDU from one of the ports of the server to the LLDP module.
- `receive` - Enables reception of LLDPDU from one of the ports of the server to the LLDP module.
- `mac-address <mac_addr>` - Configures the MAC address to be used as destination MAC address by the LLDP agent on the specified port.

Mode

Interface Configuration Mode

Default

Transmission and Reception are enabled

☞ This command executes only if lldp is started

Example

```
Your Product(config-if)# lldp transmit
```

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `show lldp interface` – Displays LLDP configuration details on a particular interface or all interfaces

- **`show lldp statistics`** – Displays the LLDP remote table statistics information.

18.12 lldp notification

Command Objective	This command controls the transmission of LLDP notifications. The no form of the command disables LLDP trap notification on an interface.

Syntax	`lldp notification [remote-table-chg][mis-configuration] [mac-address <mac_addr>]`
	
	`no lldp notification [mac-address <mac_addr>]`

Parameter **Description**	• `remote-table-chg` - Sends trap notification to NMS whenever remote table change occurs. • `mis-configuration` - Sends trap notification to NMS whenever misconfiguration is identified. • `mac-address <mac_addr>` - Configures the MAC address to be used as destination MAC address by the LLDP agent on the specified port.
Mode	Interface Configuration Mode
Default	mis-configuration
☞	This command executes only if lldp is started
Example	`Your Product(config-if)# lldp notification remote-table- chg`

Related Command(s)

- `show lldp interface` - Displays LLDP configuration details on a particular interface or all interfaces.
- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.

18.13 lldp tlv-select basic-tlv

Command Objective

This command enables the basic settings while transmitting the LLDP frames on a given port.

The no form of the command disables the basic TLV transmission on a given port.

Syntax

```
lldp tlv-select basic-tlv ( [port-descr] [sys-name] [sys- descr] [sys-capab] [mgmt-addr {all | ipv4 <ucast_addr> | ipv6 <ip6_addr>}] ) [mac-address <mac_addr>]no lldp tlv- select basic-tlv { [port-descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr {all | ipv4 <ucast_addr> | ipv6<ip6_addr>}] } [mac-address <mac_addr>]
```

Parameter Description

- `port-descr` - Configures the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).
- `sys-name` - Configures the system name of the TLV.
- `sys-descr` - Configures the system description of the TLV.
- `sys-capab` - Configures the system capabilities of the TLV.
- `mgmt-addr -` Enables the transmission on the current interface.
  - `all` - Enables the transmission of all the available management addresses on the current interface. If no management address is present/ configured in the system, switch mac-address will be taken for transmission.
  - `ipv4 <ip addr>` - Enables the transmission of a particular ipv4 address on the current interface.
  - `ipv6 <ip addr>` - Enables the transmission of a particular ipv6 address on the current interface.
- `mac-address <mac_addr>` - Configures the MAC address to be used as destination MAC address by the LLDP agent on the specified port.

Mac Address can be configured only if LLDP version is set as v2.

Mode

Interface Configuration Mode (Physical Interfaces)

☞ This command executes only if; lldp is started in the system

Example	`Your Product(config-if)# lldp tlv-select basic-tlv port- descr mgmt-addr all`

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `set lldp version` - Enables the lldp version to be used on the system.
- `show lldp local` – Displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces.

18.14 lldp port-id-subtype

Command Objective This command configures an ID for LLDP port subtype.

Syntax

```
lldp port-id-subtype { if-alias | port-comp
<string(255)> | mac-addr | if-name | local
<string(255)> }
```

Parameter

Description

- `if-alias` - Represents a chassis identifier based on the value of ifAlias for an interface on the containing chassis.
- `port-comp <string(255)>` - Represents a chassis identifier based on the value of entPhysicalAlias object for a port or backplane within the chassis.
- `mac-addr` - Represents a chassis identifier based on the value of a unicast source address, of a port on the containing chassis.
- `if-name` - Represents a chassis identifier based on the value of ifName object for an interface on the containing chassis.
- `local <string(255)>` - Represents a chassis identifier based on a locally defined value."

Mode Interface Configuration Mode

Default if-alias

☞ This command executes only if lldp is started

Example

```
Your Product(config-if)# lldp port-id-subtype mac-
addr

Your Product(config-if)# lldp port-id-subtype local
slot0/1
```

Related Command(s)

- `show lldp local` – Displays the current switch information that will be used to populate the outbound LLDP advertisements for a specific interface or all interfaces.
- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.

18.15 lldp tlv-select dot1tlv

Command Objective

This command performs dot1 TLV configuration while transmittingthe LLDP frames to the particular port apart from the basic settings.

The no form of the command disables the transmission of dot1 TLV types on a port.

Syntax

```
lldp tlv-select dot1tlv {[port-vlan-id] [protocol-vlan-id {all |<vlan-id>}] [vlan-name {all | <vlan-id>}][vid-usage- digest] [mgmt-vid] [link-aggregation]}
```

```
no lldp tlv-select dot1tlv {[port-vlan-id] [protocol-vlan- id {all |<vlan-id>}] [vlan-name {all | <vlan-id>}][vid- usage-digest] [mgmt-vid] [link-aggregation]}
```

Parameter

Description

- `port-vlan-id` - Specifies the VLAN ID of the port that uniquely identifies a specific VLAN. This VLAN ID is associated with a specific group of protocols for the specific port.
- `protocol-vlan-id` - Specifies the protocol ID that represents a specific group of protocols that are associated together when assigning a VID to a frame. This group ID is associated with the specific port.
  - `all` – Sets the protocol ID as all.
  - `<vlan-id>` - Sets the protocol id as the mentioned vlan id. This value ranges between 1 and 4094.
- `vlan-name` - Specifies the administratively assigned string, which is used to identify the VLAN.
  - `all` – Sets the protocol ID as all.
  - `<vlan-id>` - Sets the protocol id as the mentioned vlan id. This value ranges between 1 and 4094.
- `vid-usage-digest` - Performs dot1 TLV configuration while transmitting the LLDP frames to the VID usage digest TLV.


This parameter can be set only when LLDP version is set as v2.

- **mgmt-vid** - Performs dot1 TLV configuration while transmitting the LLDP frames to the managemet VID TLV.

This parameter can be set only when LLDP version is set as v2.

- **link-aggregation** - Performs dot1 TLV configuration while transmitting the LLDP frames to the link-aggregation TLV.

This parameter can be set only when LLDP version is set as v2.

Mode	Interface Configuration Mode
☞	This command executes only if lldp is started
Example	`Your Product(config-if)# lldp tlv-select dot1tlv port-vlan-id protocol-vlan-id 42`

Related Command(s)

- **no shutdown lldp** – Starts all the ports in the LLDP and releases all the allocated memory.
- **show lldp neighbors** - Displays information about the neighbors on an interface or all interfaces.
- **show lldp local** – Displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces.
- **show lldp errors** – Displays the information about the errors such as memory allocation failures, queue overflows and table overflow.
- **set lldp version** – Enables the lldp version to be used on the ports.

18.16 lldp tlv-select dot3tlv

Command Objective

This command performs dot3 TLV configuration while transmitting the LLDP frames to the particular port apart from the basic settings.

The no form of the command disables the transmission of dot3 TLV types on a port.

Syntax

```
lldp tlv-select dot3tlv { [macphy-config] [link-aggregation] [max-framesize] }
```

```
no lldp tlv-select dot3TLV { [macphy-config] [link-aggregation] [max-framesize] }
```

Parameter

Description

- `macphy-config` - Configures the physical MAC address of the TLV.
- `link-aggregation` - Configures the link aggregation protocol statistics for each port on the device.
- `max-framesize` - Configures the maximum frame size of the TLV.

Mode

Interface Configuration Mode

This command executes only if lldp is started

Example

```
Your Product(config-if)# lldp tlv-select dot3tlv macphy- config
```

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `show lldp neighbors` - Displays information about the neighbors on an interface or all interfaces.

- `show lldp local` – Displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces
- `show lldp errors` – Displays the information about the errors such as memory allocation failures, queue overflows and table overflow.

18.17 debug lldp

Command Objective

This command specifies debug level for LLDP module.

The no form of the command disables debug option for LLDP module.

Syntax

```
debug lldp [{all | init-shut| mgmt| data-path|
ctrl| pkt-dump| resource| all-fail| buf| neigh|
critical| redundancy| tlv-all| chassis-id|
port-id| ttl| port-descr| sys-name| sys-descr|
sys-capab| mgmt-addr| port-vlan| ppvlan| vlan-
name| proto-id| mac-phy| pwr-mdi| lagg| max-
frame| vid-digest| mgmt-vid| dcbx-cee }]
```

```
no debug lldp [{all | [init-shut] [mgmt] [data-
path] [ctrl] [pkt-dump] [resource] [all-fail] [buf]
[neigh] [critical][tlv {all | [chassis-id][port-id]
[ttl] [port- descr] [sys-name] [sys-descr] [sys-
capab] [mgmt-addr] [port-vlan] [ppvlan] [vlan-name]
[proto-id] [mac-phy] [pwr-mdi] [lagg] [max-frame]
[vid-digest] [mgmt-vid] [dcbx-cee]}] [redundancy]}]
```

Parameter

Description

- `all` - Generates debug statements for all traces
- `init-shut` - Generates debug statements for init and shutdown traces. This trace is generated on failed initialization and shutting down of LLDP related entries.
- `mgmt` - Generates debug statements for management traces. This trace is generated during failure in configuration of any of the LLDP features.
- `data-path` - Generates debug statements for data path traces. This trace is generated during failure in packet processing.
- `ctrl` - Generates debug statements for control path traces. This trace is generated during failure in modification or retrieving of LLDP entries
- `pkt-dump` - Generates debug statements for packet dump traces. This trace is currently not used in LLDP module.
- `resource` - Generates debug statements for OS resource related traces. This trace is generated during failure in message queues.

- **all-fail** - Generates debug statements for all failure traces of the above-mentioned traces
- **buf** - Generates debug statements for LLDP buffer related traces. This trace is currently not used in LLDP module.
- **neigh** - Generates debug statements for neighbor SEM.
- **critical** - Generates debug statements for critical SEM.
- **tlv-all** - Generates debug statements for all TLV traces
- **chassis-id** - Generates debug statements for chassis-id TLV traces
- **port-id**- Generates debug statements for port-id TLV trace
- **ttl** – Generates debug statements for TTL TLV trace
- **port-descr**- Generates debug statements for the port description TLV traces
- **sys-name**- Generates debug statements for the system name TLV traces
- **sys-descr**- Generates debug statements for system description TLV traces
- **sys-capab**- Generates debug statements for system capabilities TLV traces
- **mgmt-addr** - Generates debug statements for management address TLV traces
- **port-vlan**- Generates debug statements for port-vlan TLV traces
- **ppvlan**- Generates debug statements for port-protocol-vlan TLV traces
- **vlan-name**- Generates debug statements for vlan-name TLV traces
- **proto-id**- Generates debug statements for protocol-id TLV traces
- **mac-phy**- Generates debug statements for MAC or PHY TLV traces
- **pwr-mdi**- Generates debug statements for power-through-MDI TLV traces
- **lagg** - Generates debug statements for link aggregation TLV traces
- **max-frame** - Generates debug statements for maximum frame size TLV traces
- **vid-digest**- Generates debug statements for vid digest TLV traces
- **mgmt-vid**- Generates debug statements for management VID TLV traces
- **dcbx-cee**- Generates debug statements for dcbx (cee) TLV traces
- **redundancy** - Generates the debug statements for the LLDP redundancy module.

Mode Privileged Exec Mode

☞ This command executes only if lldp is started

Example

```
Your Product# debug lldp init-shut

Your Product# debug lldp tlv-all
```

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.

18.18 show lldp

Command Objective	This command displays LLDP global configuration details to initialize on an interface.
Syntax	`show lldp`
Mode	Privileged EXEC Mode
☞	This command executes only if lldp is started

Example

```
Your Product# show lldp
LLDP is enabled
LLDP Version: v2
Transmit Interval: 20
Holdtime Multiplier: 4
Reinitialization Delay: 2
Tx Delay: 2
Notification Interval: 30
TxCreditMax: 5
MessageFastTx: 1
TxFastInit: 4
Chassis Id SubType: Chassis Component
Chassis Id: Aricentswitch
```

Related Command(s)

- `set lldp` – Enables or disables LLDP on the system.
- `lldp transmit-interval` – Sets the transmission interval
- `lldp holdtime-multiplier` - Sets the multiplier value
- `lldp reinitialization-delay` - Sets the reinitialization delay

- **lldp tx-delay** - Sets the transmit delay
- **lldp notification-interval** - Sets the notification interval
- **lldp chassis-id-subtype** - Configures lldp chassis id subtype and chassis id value
- **no shutdown lldp** – Starts all the ports in the LLDP and releases all the allocated memory.
- **set lldp version** – Enables the lldp version to be used on the system.
- **lldptxCreditMax** – Configures the maximum number of consecutive LLDPDUs that can be transmitted any time
- **lldp MessageFaxtTx** – Configures the interval at which LLDP frames are transmitted on behalf of this LLDP agent during fast transmission period
- **lldp txFastInit** - Configures the value used to initialize the txFast variable which determines the number of transmissions that are made in fast transmission mode

18.19 show lldp interface

Command Objective

This command displays the information about interfaces where LLDP is enabled

Syntax

```
show lldp interface [<interface-type> <interface-id>] [mac-address <mac_addr>]
```

Parameter Description

- `<interface-type>` - Displays the information about the specified type of interface. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Displays the information about the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For Example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. ForExample: 1 represents port-channel ID.
- `mac-address <mac_addr>` - Displays information about neighbors for the specidfied destination MAC address of the LLDP agent

Mode

Privileged EXEC Mode

☞ This command executes only if lldp is started

Example

```
Your Product# show lldp interface gigabitethernet 0/1

Gi0/1:

Tx State: Enabled
```

```
Rx State: Enabled
Tx SEM State: INITIALIZE
Rx SEM State: INITIALIZE
Notification Status: Disabled
Notification Type: Mis-configuration
DestinationMacAddr : 01:80:c2:00:00:0e
```

Related Command(s)

- **`set lldp`** - Enables or disables LLDP on the system
- **`lldp transmit / receive`** – Sets LLDP admin status on an interface to Transmit or Receive
- **`lldp notification`** – Enables LLDP trap notification on an interface
- **`no shutdown lldp`** – Starts all the ports in the LLDP and releases all the allocated memory.
- **`lldp dest-mac`** - Configures destination mac-address to be used by the LLDP agent for transmission on this port.

18.20 show lldp neighbors

Command Objective

This command displays information about neighbors on an interface or all interfaces.

Syntax

```
show lldp neighbors [chassis-id <string(255)> port-I
<string(255)>] [<interface-type> <interface-
id>][detail]
```

Parameter

Description

- `chassis-id <string(255)>` - DisplaysLLDP Neighbor information for the specified chassis identifier value this value is a string value with a maximum size of 255.
- `port-id <string(255)>` - DisplaysLLDP Neighbor information for the specified port number that represents the concerned aggregation port. This value is a string value with a maximum size of 255.
- `<interface-type>` - Displays information about neighbors for the specified type of interface. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-id>` - Displays information about neighbors for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For Example: 0/1 represents that the slot number is 0 and port number is 1. Onl port-channel ID is provided, for interface type port-channel. For Example: 1 represents port-channel ID.
- `detail` - Displays the information obtained from all the received TLVs

Mode

Privileged EXEC Mode

☞ This command can be executed only if LLDP is started

Example

```
Your Product# show LLDP neighbors
Capability Codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable
Device, (W) WLAN Access Point, (P) Repeater, (S) Station, (O)
Other
Chassis ID      Local Intf  Hold-time   Capability   Port Id
----------     ----------  ---------    ----------    -------
00:01:02:03:04:01  Gi0/1      120        B,R         Slot0/1
00:02:02:03:04:01  Gi0/2      120                    Slot0/3
00:02:02:03:04:01  Gi0/3      120                    Slot0/2
00:01:02:03:04:01  Gi0/2      120                    Slot0/2
00:01:02:03:04:01  Gi0/3      120                    Slot0/2
Total Entries Displayed : 5
Your Product# show lldp neighbors chassis-id
00:01:02:03:04:01 port-id Slot0/2
Capability Codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable
Device, (W) WLAN Access Point, (P) Repeater, (S) Station, (O)
Other
Chassis ID        Local  Intf   Hold-time  Capability   Port Id
----------        ----------   ---------  ----------    -----
00:01:02:03:04:01  Gi0/2        120                     Slot0/2
00:01:02:03:04:01  Gi0/3        120                     Slot0/2
Total Entries Displayed: 2
Your Product# show lldp neighbors chassis-id
00:01:02:03:04:01 port-id Slot0/2 gigabitethernet 0/2
Capability Codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable
Device,(W) WLAN Access Point, (P) Repeater, (S) Station, (O)
Other
```

```
Chassis ID       Local Intf  Hold-time   Capability        Port Id
----------       ----------  ---------   ----------        ----
00:01:02:03:04:01Gi0/2       120                           1
Total Entries Displayed
```

Your Product# show lldp neighbors chassis-id

00:01:02:03:04:01 port-id Slot0/2 detail

```
Capability Codes:

(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable

Device, (W) WLAN Access Point, (P) Repeater, (S) Station, (O)
Other

Chassis Id SubType: Mac Address

Chassis Id: 00:01:02:03:04:01

Port Id SubType: Interface Alias

Port Id: Slot0/2

Port Description: Not Advertised

System Name: Not Advertised

System Desc: Not Advertised

Local Intf: Gi0/2

Time Remaining: 92 Seconds

System Capabilities Tlv: Not Advertised
Management Addresses: Not Advertised Extended
802.3 TLV Info

-MAC PHY Configuration & Status
Auto Negotiation Tlv: Not Advertised

-Link Aggregation

Link Aggregation Tlv: Not Advertised

-Maximum Frame Size Tlv: Not Advertised

Extended 802.1 TLV Info

-Port VLAN Id: 0
```

```
-Port & Protocol VLAN Id

Protocol Vlan Tlv: Not Advertised

-Vlan Name

Vlan Id Vlan Name

Chassis Id SubType: Mac Address

Chassis Id: 00:01:02:03:04:01

Port Id SubType: Interface Alias

Port Id: Slot0/2

Port Description: Not Advertised

System Name: Not Advertised

System Desc: Not Advertised

Local Intf: Gi0/3

Time Remaining: 92 Seconds

System Capabilities Tlv: Not Advertised
Management Addresses: Not Advertised

Extended 802.3 TLV Info

-MAC PHY Configuration & Status

Auto Negotiation Tlv: Not Advertised

-Link Aggregation

Link Aggregation Tlv: Not Advertised


-Maximum Frame Size Tlv: Not Advertised

Extended 802.1 TLV Info

-Port VLAN Id: 0

-Port & Protocol VLAN Id

Protocol Vlan Tlv: Not Advertised

-Vlan Name

Vlan Id        Vlan Name
```

```
Total Entries Displayed: 2

Your Product# show lldp neighbors gigabitethernet 0/1 detail

Capability Codes:

(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable

Device, (W) WLAN Access Point, (P) Repeater, (S) Station,
(O) Other

Chassis Id SubType: Mac Address

Chassis Id: 00:01:02:03:04:01

Port Id SubType: Interface Alias

Port Id: Slot0/1

Port Description: Ethernet Interface

System Name: SMIS

System Desc: SNMPV2

Local Intf: Gi0/1

Time Remaining: 95 Seconds

System Capabilities Supported: B,R
System Capabilities Enabled: B,R
Management Addresses: IfId

Extended 802.3 TLV Info

-MAC PHY Configuration & Status

Auto-Neg Support & Status: Supported, Disabled

Advertised Capability Bits: 8000

Other

-Link Aggregation

Capability & Status: Not Capable, Not In

Aggregation

Aggregated Port Id: 1

-Maximum Frame Size: 1500
```

```
Extended 802.1 TLV Info

-Port VLAN Id: 1

-Port & Protocol VLAN Id

Protocol Vlan Id          Support        Status

----------------          -------        ------

1                         Supported      Enabled

2                         Supported      Enabled

30                        Supported      Enabled

-Vlan Name

Vlan Id        Vlan Name

-------        ---------

1              vlan1

2              vlan2

30             vlan30

------------------------------------------------------------

Total Entries Displayed : 1
```

Related Command(s)

- **no shutdown lldp** – Starts all the ports in the LLDP and releases all the allocated memory.
- **set lldp** - Enables or disables LLDP on the system
- **clear lldp table** – Clears all the LLDP table of information about the neighbors.
- **lldp tlv-select basic-tlv** – Configures basic TLV types to be transmitted on a given port
- **lldp tlv-select dot1tlv** – Configures dot1 TLV types to be transmitted on a port
- **lldp tlv-select dot3tlv** - Configures dot3 TLV types to be transmitted on a port

---

18.21 show lldp traffic

Command Objective

This command displays LLDP counters on all interfaces or on a specific interface. This includes the following:

- Total Frames Out
- Total Entries Aged
- Total Frames In
- Total Frames Received In Error
- Total Frames Discarded
- Total TLVS Unrecognized
- Total TLVs Discarded

Syntax

```
show lldp traffic [<iftype> <ifnum>[mac-address <mac_addr>]]
```

Parameter

Description

- `<iftype>` - Displays the LLDP counters for specified type of interface. Th interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer upto
- 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<ifnum>` - Displays the LLDP counters for specified interface identifier.
- This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For Example: 0/1represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. ForExample: 1 represents port-channel ID
- `mac-address <mac_addr>` - Displays information about neighbors for the specidfied destination MAC address of the LLDP agent

Mode Privileged EXEC Mode

☞ This command executes only if lldp is started

Example

```
Your Product# show lldp traffic
Total Frames Out: 107
Total Entries Aged: 0
Total Frames In: 159
Total Frames Received In Error: 0
Total Frames Discarded: 0
Total TLVS Unrecognized: 0
Total TLVs Discarded: 0
Your Product# show lldp traffic gigabitethernet 0/1
Total Frames Out: 49
Total Entries Aged: 0
Total Frames In: 42
Total Frames Received In Error: 0
Total Frames Discarded: 0
Total TLVS Unrecognized: 0
Total TLVs Discarded: 0
Total PDU length error Drops: 0
```

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `set lldp` - Enables or disables LLDP on the system
- `clear lldp counters` – Clears the entire interface related transmit and receive counters.

18.22 show lldp local

Command Objective

This command displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces.

Syntax

```
show lldp local {[<interface-type> <interface-id>
[mac- address <mac_addr>]] | [mgmt-addr]}
```

Parameter

Description

- `<interface-type>` - Displays the current switch information for the specified type of interface. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together
- `<interface-id>` - Displays the current switch information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For Example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. For Example: 1 represents port-channel ID.
- `mac-address <mac_addr>` - Displays information about neighbors for the specidfied destination MAC address of the LLDP agent
- `mgmt-addr` - All the management addresses configured in the system and Tx enabled ports

Mode

Privileged EXEC Mode

This command can be executed only if lldp is started

Example

```
Your Product# show lldp local

Capability Codes:

(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable

Device, (W) WLAN Access Point, (P) Repeater, (S) Station, (O)
Other

Chassis Id SubType: Mac Address

Chassis Id: 00:02:02:03:04:01

System Name: SMIS

System Description: SNMPV2

System Capabilities Supported: B,R
System Capabilities Enabled: B,R

Gi0/1 :

Port Id SubType: Interface Alias

Port Id: Gi0/1

Port Description: Ethernet Interface Port 01

Enabled Tx Tlvs: Port Description, System

Description,

Management Address

Extended 802.3 TLV Info

-MAC PHY Configuration & Status Auto-Neg
Support & Status:  , Advertised
Capability Bits: b24e Other

10base-T(FD)

100base-T4

100base-T2(HD) Asym
PAUSE(FD)

1000base-X, -LX, -SX, -CX(HD)

1000base-X, -LX, -SX, -CX(FD)

1000base-T(HD)
```

```
Operational MAU Type: 0
-Link Aggregation
Capability & Status: Not Capable, Not In
Aggregation
Aggregated Port Id: 0
-Maximum Frame Size: 1500
Extended 802.1 TLV Info
-Port VLAN Id: 1
-Port & Protocol VLAN Id
Protocol VLAN Id   Support    Protocol VLAN Status   TxStatus
----------------   -------    -----------------     --------
0                  Supported  Enabled                Disabled
1                  Supported  Enabled                Disabled
-Vlan Name   Vlan Id  -VID TLV:  VID      TxStatus
----------   -------  ---------  -------  ---------
 0 Disabled Vid TLV: TxStatus Management 1 Disabled
------------------------------------------------------------
```

Your Product# show lldp local gigabitethernet 0/1

```
Port Id SubType: Interface Alias
Port Id: Slot0/1
Port Description: Ethernet Interface
Enabled Tx Tlvs: Port Description, System Name,
      System Description, System Capability, Management
      Address, Port Vlan, MacPhy,
Link Aggregation, Max Frame Size
       Extended 802.3 TLV Info
       -MAC PHY Configuration & Status
Auto-Neg Support & Status: Supported, Disabled
```

```
Advertised Capability Bits: 8000

Other

Operational MAU Type: 0

      -Link Aggregation

Capability & Status: Not Capable, Not In

Aggregation

Aggregated Port Id: 1

      -Maximum Frame Size: 1500

Extended 802.1 TLV Info

      -Port VLAN Id: 1

      -Port & Protocol VLAN Id

Protocol VLAN Id   Support    Protocol VLAN Status TxStatus

----------------   -------    -------- ----------- -----

0                  Supported  Enabled              Enabled

-------------------------------------------------------------
```

Your Product# show lldp local mgmt-addr

```
Management Address              TxEnabledPorts

------------------              --------------

13.0.0.1                        Gi0/1

15.0.0.1                        Gi0/1
```

Related Command(s)

- **no shutdown lldp** – Starts all the ports in the LLDP and releases all the allocated memory.
- **set lldp** - Enables or disables LLDP on the system
- **lldp chassis-id-subtype** - Configures lldp chassis id subtype and chassis id value
- **lldp port-id-subtype** - Configures lldp port id subtype and port id value for a given port
- **lldp tlv-select basic-tlv** – Configures basic TLV types to be transmitted on a given port

- `lldp tlv-select dot1tlv` – Configures dot1 TLV types to be transmitted on a port
- `lldp tlv-select dot3tlv` - Configures dot3 TLV types to be transmitted on a port

18.23 show lldp errors

Command Objective	This command displays the information about the errors such as memory allocation failures, queue overflows and table overflow.
Syntax	`show lldp errors`
Mode	Privileged EXEC Mode

Example	`Your Product# show lldp errors`
	`Total Memory Allocation Failures: 0`
	`Total Input Queue Overflows: 0`
	`Total Table Overflows: 0`

☞	This command can be executed only if lldp is started

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `set lldp` - Enables or disables LLDP on the system
- `lldp tlv-select basic-tlv` – Configures basic TLV types to be transmitted on a given port
- `lldp tlv-select dot1tlv` – Configures dot1 TLV types to be transmitted on a port
- `lldp tlv-select dot3tlv` - Configures dot3 TLV types to be transmitted on a port

18.24 show lldp statistics

Command Objective This command displays the LLDP remote table statistics information.

Syntax `show lldp statistics`

Mode Privileged EXEC Mode

Example

```
Your Product# show lldp statistics

Remote Table Last Change Time: 100300

Remote Table Inserts: 5

Remote Table Deletes: 0

Remote Table Drops: 0

Remote Table Ageouts: 0

Remote Table Updates: 4
```

☞ This command can be executed only if lldp is started

Related Command(s)

- `set lldp` - Enables or disables LLDP on the system
- `lldp transmit / receive` - Sets LLDP admin status on an interface to transmit / receive
- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.

18.25 lldp dest-mac

Command Objective	This command configures destination mac-address to be used by the LLDP agent for transmission on this port. The no form of the command resets the destination mac-address to LLDP multicast address.

Syntax	`lldp dest-mac <mac_addr>`
	
	`no lldp dest-mac <mac_addr>`

Mode	Interface Configuration Mode (Physical Interfaces)
Default	The default value would the LLDP multicast MAC address
☞	This command can be executed only if lldp is started. Version 1 support 01:80:C2:00:00:0E only. Version 2 support 01:80:C2:00:00:0E, 01:80:C2:00:00:00 and 01:80:C2:00:00:03.
Example	`Your Product(config-if)# lldp dest-mac 00:11:22:33:44:55`
Related Command(s)	• `no shutdown lldp` – . Enables all the ports by allocating the required resources in the LLDP. • `show lldp interface` - Displays the information about interfaces where LLDP is enabled

18.26 set lldp version

Command Objective This command enables the lldp version to be used on the system.

Syntax `set lldp version {v1 | v2}`

Parameter

Description

- `v1 - Enables LLDP 2005 version 1 on the port`
- `v2 - Enables LLDP 2009 version 2 on the port`

Mode Global Configuration Mode

Default v1

☞ This command executes only if lldp is disabled. All LLDP configuration is reset to default after version change.

Example

```
Your Product(config)# set lldp version v1
```

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `show lldp` - Displays LLDP global configuration details to initialize on an interface

18.27 lldp txCreditMax

Command Objective	This command configures the maximum number of consecutive LLDPDUs that can be transmitted any time. This value ranges between 1 and 10.
Syntax	`lldp txCreditMax <value (1-10)>`
Mode	Global Configuration Mode
Default	5
☞	This command executes only if lldp is started and version is v2.
Example	`Your Product(config)# lldp txCreditMax 3`

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `show lldp` - Displays LLDP global configuration details to initialize on an interface

18.28 lldp MessageFastTx

Command Objective	This command configures the interval at which LLDP frames are transmitted on behalf of this LLDP agent during fast transmission period. This value ranges between 1 and 3600 seconds.
Syntax	`lldp MessageFastTx <seconds(1-3600)>`
Mode	Global Configuration Mode
Default	1
☞	This command executes only if lldp is started and version is v2.
Example	`Your Product(config)# lldp MessageFastTx 3500`
Related Command(s)	• `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory. • `show lldp` - Displays LLDP global configuration details to initialize on an interface

18.29 lldp txFastInit

Command Objective	This command configures the value used to initialize the txFast variable which determines the number of transmissions that are made in fast transmission mode. This value ranges between 1 and 8.
Syntax	`lldp txFastInit <value (1-8)>`
Mode	Global Configuration Mode
Default	4
☞	This command executes only if lldp is started and version is v2.
Example	`Your Product(config)# lldp txFastInit 3`
Related Command(s)	• `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory. • `show lldp` - Displays LLDP global configuration details to initialize on an interface

18.30 show lldp peer

Command Objective	This command displays information about the peers on an interface or all interfaces.

Syntax

```
show lldp peers [chassis-id <string(255)> port-id <string(255)>] <interface-type> <interface-id>[[mac-address <mac_addr>] [detail]]
```

Parameter Description

- `chassis-id <string(255)>` - Displays the LLDP peer information for the specified chassis identifier. This value is a string of maximum size 255.
- `port-id <string(255)>` - Displays the port number that represents the concerned aggregation port This value is a string of maximum size 255.
- `<interface-type>` - Displays information about LLDP peers for the specified type of interface. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-id>` - Displays information about peers for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel.For Example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. For Example: 1represents port-channel ID.
- `mac-address <mac_addr>` - Displays information about peers for the specidfied destination MAC address of the LLDP agent
- `detail` - Displays the information obtained from all the received TLVs.

Mode Privileged EXEC Mode

☞ This command can be executed only if lldp is started

Example

```
Your Product # show lldp peers gigabitethernet 0/1
Capability Codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Chassis ID          Local Intf    Hold-time     Capability    Port   Id
---------           ---------     ---------     ---------     ----   --
00:01:02:03:04:01 Gi0/1    120           B,R           Slot0/1
```

Related Command(s)

- **no shutdown lldp** – Starts all the ports in the LLDP and releases all the allocated memory.
- **set lldp** - Enables or disables LLDP on the system
- **clear lldp table** – Clears all the LLDP table of information about the neighbors.
- **lldp tlv-select basic-tlv** – Configures basic TLV types to be transmitted on a given port
- **lldp tlv-select dot1tlv** – Configures dot1 TLV types to be transmitted on a port
- **lldp tlv-select dot3tlv** - Configures dot3 TLV types to be transmitted on a port

---

Contacting Supermicro

Headquarters

Address:	Super Micro Computer, Inc. 980 Rock Ave. San Jose, CA 95131 U.S.A.
Tel:	+1 (408) 503-8000
Fax:	+1 (408) 503-8008
Email:	marketing@supermicro.com (General Information) support@supermicro.com (Technical Support)
Web Site:	www.supermicro.com

Europe

Address:	Super Micro Computer B.V. Het Sterrenbeeld 28, 5215 ML 's-Hertogenbosch, The Netherlands
Tel:	+31 (0) 73-6400390
Fax:	+31 (0) 73-6416525
Email:	sales@supermicro.nl (General Information) support@supermicro.nl (Technical Support) rma@supermicro.nl (Customer Support)
Web Site:	www.supermicro.com.nl

Asia-Pacific

Address:	Super Micro Computer, Inc. 3F, No. 150, Jian 1st Rd. Zhonghe Dist., New Taipei City 235 Taiwan (R.O.C)
Tel:	+886-(2) 8226-3990
Fax:	+886-(2) 8226-3992
Email:	support@supermicro.com.tw
Web Site:	www.supermicro.com.tw