Supermicro Switch Configuration CLI Guide

Supermicro.com

SMIS Supermicro.com

CLI User Manual_Vol1
## Contents

**CHAPTER 1: INTRODUCTION**
- 1.1 PURPOSE .................................................................................. 11
- 1.2 SCOPE .................................................................................... 11
- 1.3 DOCUMENT CONVENTIONS ..................................................... 11
- 1.4 INDUSTRY STANDARD CLI ...................................................... 12
- 1.5 KEY CONVENTIONS ............................................................... 12

**CHAPTER 2: COMMAND LINE INTERFACE** ........................................ 13
- 2.1 CONTEXT SENSITIVE HELP ...................................................... 14
- 2.2 CLI COMMAND MODES .......................................................... 15
- 2.2.1 User EXEC Mode ............................................................... 17
- 2.2.2 Privileged EXEC Mode ....................................................... 17
- 2.2.3 Global Configuration Mode ................................................ 17
- 2.2.4 Interface Configuration Mode ............................................. 17
- 2.2.5 Physical Interface Mode ..................................................... 17
- 2.2.5.1 Port Channel Interface Mode ........................................... 17
- 2.2.5.2 VLAN Interface Mode .................................................... 17
- 2.2.5.3 Management Interface Mode .......................................... 17
- 2.2.6 Interface Range Mode ....................................................... 18
- 2.2.7 Config-VLAN Mode ........................................................... 18
- 2.2.8 Line Configuration Mode .................................................... 18
- 2.2.9 Protocol Specific Modes .................................................... 18
- 2.2.9.1 VRRP Router Configuration Mode ................................... 19
- 2.2.9.2 VRRP Interface Configuration Mode ................................ 19
- 2.2.9.3 DHCP Pool Configuration Mode ..................................... 19
- 2.2.9.4 SNTP Configuration Mode .............................................. 19
- 2.2.9.5 MSTP Configuration mode ............................................. 19
- 2.2.9.6 DiffSrv ClassMap Configuration mode .............................. 19
- 2.2.9.7 DiffSrv Policy-Map Configuration Mode ............................ 21
- 2.2.9.8 ACL Standard Access List Configuration Mode .................. 21
- 2.2.9.9 ACL Extended Access List Configuration Mode ............... 21
- 2.2.9.10 ACL MAC Configuration Mode ..................................... 21

**CHAPTER 3: SYSTEM COMMANDS** ..................................................... 23
- 3.1 HELP .................................................................................... 25
- 3.2 CLEAR SCREEN .................................................................... 26
- 3.3 ENABLE .............................................................................. 27
- 3.4 DISABLE ............................................................................. 28
- 3.5 CONFIGURE TERMINAL ....................................................... 29
- 3.6 CONFIGURE ....................................................................... 30
- 3.7 RUN SCRIPT ........................................................................ 31
- 3.8 LISTUSER ........................................................................... 32
- 3.9 LOCK ................................................................................. 33
- 3.10 USERNAME ........................................................................ 34
- 3.11 ENABLE PASSWORD .......................................................... 36
- 3.12 LINE ................................................................................. 37
- 3.13 ALIAS - REPLACEMENT STRING ......................................... 38
- 3.14 ALIAS – INTERFACE | EXEC | CONFIGURE .......................... 39
- 3.15 ACCESS-LIST PROVISION MODE ....................................... 40
- 3.16 ACCESS-LIST COMMIT ........................................................ 41
- 3.17 EXEC-TIMEOUT .................................................................. 42
- 3.18 LOGOUT .............................................................................. 43
- 3.19 END .................................................................................. 44
- 3.20 EXIT .................................................................................. 45
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>DEFAULT MODE .................................................. 65</td>
</tr>
<tr>
<td>4.2</td>
<td>DEFAULT RESTORE-FILE ........................................ 66</td>
</tr>
<tr>
<td>4.3</td>
<td>IP ADDRESS ...................................................... 67</td>
</tr>
<tr>
<td>4.4</td>
<td>SWITCHPORT ...................................................... 69</td>
</tr>
<tr>
<td>4.5</td>
<td>IP ADDRESS - RARP/DHCP ...................................... 71</td>
</tr>
<tr>
<td>4.6</td>
<td>LOGIN AUTHENTICATION .......................................... 73</td>
</tr>
<tr>
<td>4.7</td>
<td>LOGIN AUTHENTICATION-DEFAULT .................................. 74</td>
</tr>
<tr>
<td>4.8</td>
<td>AUTHORIZED-MANAGER IP-SOURCE .................................. 75</td>
</tr>
<tr>
<td>4.9</td>
<td>IP HTTP PORT .................................................... 77</td>
</tr>
<tr>
<td>4.10</td>
<td>SET IP HTTP ..................................................... 78</td>
</tr>
<tr>
<td>4.11</td>
<td>MTU ................................................................. 79</td>
</tr>
<tr>
<td>4.12</td>
<td>SYSTEM MTU ........................................................ 80</td>
</tr>
<tr>
<td>4.13</td>
<td>BRIDGE PORT-TYPE ................................................ 81</td>
</tr>
<tr>
<td>4.14</td>
<td>SYSTEM-SPECIFIC PORT-ID ....................................... 84</td>
</tr>
<tr>
<td>4.15</td>
<td>SET CUSTOM-PARAM ................................................. 85</td>
</tr>
<tr>
<td>4.16</td>
<td>MAC-ADDR .......................................................... 86</td>
</tr>
<tr>
<td>4.17</td>
<td>SNMP TRAP LINK-STATUS .......................................... 87</td>
</tr>
<tr>
<td>4.18</td>
<td>WRITE ............................................................... 88</td>
</tr>
<tr>
<td>4.19</td>
<td>COPY ................................................................. 89</td>
</tr>
<tr>
<td>4.20</td>
<td>COPY STARTUP-CONFIG ............................................. 90</td>
</tr>
<tr>
<td>4.21</td>
<td>COPY RUNNING-CONFIG STARTUP-CONFIG .......................... 91</td>
</tr>
<tr>
<td>4.22</td>
<td>COPY LOGS .......................................................... 92</td>
</tr>
<tr>
<td>4.23</td>
<td>FIRMWARE UPGRADE ................................................ 93</td>
</tr>
<tr>
<td>4.24</td>
<td>COPY - FILE ........................................................ 94</td>
</tr>
<tr>
<td>4.25</td>
<td>CLOCK SET .......................................................... 95</td>
</tr>
<tr>
<td>4.26</td>
<td>ERASE ............................................................... 96</td>
</tr>
<tr>
<td>4.27</td>
<td>CLI CONSOLE ........................................................ 97</td>
</tr>
<tr>
<td>4.28</td>
<td>FLOWCONTROL ....................................................... 98</td>
</tr>
<tr>
<td>4.29</td>
<td>TUNNEL MODE ....................................................... 100</td>
</tr>
<tr>
<td>4.30</td>
<td>TUNNEL CHECKSUM ................................................ 101</td>
</tr>
<tr>
<td>4.31</td>
<td>TUNNEL PATH-MTU-DISCOVERY .................................... 102</td>
</tr>
<tr>
<td>4.32</td>
<td>TUNNEL UDLR ....................................................... 103</td>
</tr>
<tr>
<td>4.33</td>
<td>SHUTDOWN - PHYSICAL/VLAN/PORT-CHANNEL/TUNNEL INTERFACE ........................................... 104</td>
</tr>
<tr>
<td>4.34</td>
<td>DEBUG INTERFACE .................................................. 105</td>
</tr>
<tr>
<td>4.35</td>
<td>DEBUG-LOGGING .................................................... 106</td>
</tr>
<tr>
<td>4.36</td>
<td>INCREMENTAL-SAVE ................................................. 107</td>
</tr>
<tr>
<td>4.37</td>
<td>AUTO-SAVE TRIGGER ................................................ 108</td>
</tr>
<tr>
<td>4.38</td>
<td>SET SWITCH MAXIMUM - THRESHOLD .............................. 109</td>
</tr>
<tr>
<td>4.39</td>
<td>SET SWITCH TEMPERATURE - THRESHOLD ......................... 110</td>
</tr>
</tbody>
</table>
4.40 SET SWITCH POWER - THRESHOLD ...................................................... 111
4.41 MAC-LEARN-RATE ........................................................................ 112
4.42 SYSTEM CONTACT ........................................................................ 114
4.43 SYSTEM LOCATION ......................................................................... 115
4.44 CLEAR INTERFACES - COUNTERS .............................................. 116
4.45 CLEAR COUNTERS .......................................................................... 117
4.46 SHOW IP INTERFACE ...................................................................... 118
4.47 SHOW AUTHORIZED-MANAGERS ................................................ 120
4.48 SHOW INTERFACES ......................................................................... 121
4.49 SHOW INTERFACES - COUNTERS .................................................. 125
4.50 SHOW SYSTEM-SPECIFIC PORT-ID ............................................ 128
4.51 SHOW CUSTOM-PARAM ................................................................. 129
4.52 SHOW INTERFACE MTU ................................................................. 130
4.53 SHOW INTERFACE BRIDGE PORT-TYPE .................................... 132
4.54 SHOW NVRAM ................................................................................ 134
4.55 SHOW ENV ..................................................................................... 136
4.56 SHOW SYSTEM INFORMATION ..................................................... 138
4.57 SHOW FLOW-CONTROL ................................................................. 139
4.58 SHOW DEBUG-LOGGING ............................................................... 140
4.59 SHOW DEBUGGING ........................................................................ 141
4.60 SHOW CLOCK ................................................................................ 142
4.61 SHOW RUNNING-CONFIG ............................................................. 143
4.62 SHOW HTTP SERVER STATUS .................................................... 150
4.63 SHOW SYSTEM ACKNOWLEDGEMENT ....................................... 151
4.64 SHOW MAC-LEARN-RATE ............................................................. 152
4.65 PORT-ISOLATION IN_VLAN_ID .................................................. 153
4.66 SHOW PORT-ISOLATION ............................................................... 154
4.67 PRIVATE-VLAN MAPPING ............................................................. 155
4.68 AUDIT-LOGGING ........................................................................... 156
4.69 AUDIT-LOGGING FILENAME ...................................................... 157
4.70 AUDIT-LOGGING FILESIZE .......................................................... 158
4.71 AUDIT-LOGGING RESET .............................................................. 159
4.72 SHOW CONFIG LOG ...................................................................... 160
4.73 HOL BLOCKING PREVENTION ...................................................... 161
4.74 INTERNAL-LAN .............................................................................. 162
4.75 SHOW INTERNAL-LAN ................................................................. 163
4.76 SHOW IFTYPE PROTOCOL DENY TABLE .................................... 164
4.77 CLEAR LINE VTY .......................................................................... 165
4.78 TUNNEL HOP-LIMIT ...................................................................... 166
4.79 LOGIN BLOCK-FOR ........................................................................ 167
4.80 AUDIT-LOGGING LOGSIZE-THRESHOLD .................................. 168
4.81 FEATURE TELNET ........................................................................... 169
4.82 SHOW TELNET SERVER ............................................................... 170
4.83 SHOW AUDIT ................................................................................ 171
4.84 SET HTTP AUTHENTICATION-Scheme ........................................ 172
4.85 SET HTTP REDIRECTION ENABLE .......................................... 173
4.86 HTTP REDIRECT ........................................................................... 174
4.87 SHOW HTTP AUTHENTICATION-Scheme .................................... 175
4.88 SHOW HTTP REDIRECTION ........................................................ 176
4.89 ENTITY MIB ................................................................................... 177
4.89.1 set entity physical-index ............................................................ 178
4.89.2 show entity logical ................................................................. 180
4.89.3 show entity physical ............................................................... 181
4.89.4 show entity lp-mapping ........................................................... 182
4.89.5 show entity alias-mapping ...................................................... 183
4.89.6 show entity phy-containment ................................................ 184
### CHAPTER 9: SNTP

| 9.1 | SNTP .................................................................................................................. 245 |
| 9.2 | SET SNTP CLIENT ................................................................................................. 247 |
| 9.3 | SET SNTP CLIENT VERSION .................................................................................. 249 |
| 9.4 | SET SNTP CLIENT ADDRESSING MODE ................................................................ 250 |
| 9.5 | SET SNTP CLIENT PORT ........................................................................................ 250 |
| 9.6 | SET SNTP CLIENT CLOCK-FORMAT ....................................................................... 251 |
| 9.7 | SET SNTP CLIENT TIME ZONE ............................................................................... 253 |
| 9.8 | SET SNTP CLIENT CLOCK-SUMMER-TIME ............................................................ 254 |
| 9.9 | SET SNTP CLIENT AUTHENTICATION-KEY ............................................................ 256 |
| 9.10 | SET SNTP UNICAST-SERVER AUTO-DISCOVERY .................................................. 257 |
| 9.11 | SET SNTP UNICAST-POLL-INTERVAL ................................................................... 258 |
| 9.12 | SET SNTP UNICAST-MAX-POLL-TIMEOUT ............................................................ 259 |
| 9.13 | SET SNTP UNICAST-MAX-POLL-RETRY ................................................................. 260 |
| 9.14 | SET SNTP UNICAST-SERVER .................................................................................. 261 |
| 9.15 | SET SNTP BROADCAST-MODE SEND-REQUEST .................................................. 262 |
| 9.16 | SET SNTP BROADCAST-POLL-TIMEOUT ............................................................... 263 |
| 9.17 | SET SNTP BROADCAST-DELAY-TIME ................................................................... 264 |
| 9.18 | SET SNTP MULTICAST-MODE SEND-REQUEST .................................................... 265 |
| 9.19 | SET SNTP MULTICAST-POLL-TIMEOUT ................................................................ 266 |
| 9.20 | SET SNTP MULTICAST-DELAY-TIME ................................................................... 267 |
| 9.21 | SET SNTP MULTICAST-GROUP-ADDRESS ............................................................ 268 |
| 9.22 | SET SNTP MANCAST-POLL-INTERVAL .................................................................. 269 |
| 9.23 | SET SNTP MANCAST-POLL-TIMEOUT ................................................................... 270 |
| 9.24 | SET SNTP MANCAST-POLL-RETRY-COUNT .......................................................... 271 |
| 9.25 | SET SNTP MANCAST-SERVER ............................................................................... 272 |
| 9.26 | SHOW SNTP CLOCK .............................................................................................. 273 |
| 9.27 | SHOW SNTP STATUS ............................................................................................. 274 |
| 9.28 | SHOW SNTP UNICAST—MODE STATUS .................................................................. 275 |
| 9.29 | SHOW SNTP BROADCAST—MODE STATUS .............................................................. 276 |
| 9.30 | SHOW SNTP MULTICAST—MODE STATUS ............................................................... 277 |
| 9.31 | SHOW SNTP MANCAST—MODE STATUS ................................................................. 278 |
| 9.32 | DEBUG SNTP ......................................................................................................... 279 |
| 9.33 | SHOW SNTP STATISTICS ...................................................................................... 280 |

### CHAPTER 10: SNMPV3

| 10.1 | ENABLE SNMPSUBAGENT ....................................................................................... 283 |
| 10.2 | DISABLE SNMPSUBAGENT .................................................................................... 285 |
| 10.3 | ENABLE SNMPAGENT ........................................................................................... 286 |
| 10.4 | DISABLE SNMPAGENT .......................................................................................... 287 |
| 10.5 | SNMP COMMUNITY INDEX ................................................................................... 288 |
| 10.6 | SNMP GROUP ........................................................................................................ 289 |
| 10.7 | SNMP ACCESS ....................................................................................................... 290 |
| 10.8 | SNMP ENGINEID .................................................................................................. 291 |
| 10.9 | SNMP PROXY NAME ............................................................................................ 292 |
| 10.10 | SNMP MIBPROXY NAME ..................................................................................... 293 |
| 10.11 | SNMP VIEW .......................................................................................................... 294 |
| 10.12 | SNMP TARGETADDR ............................................................................................ 295 |
| 10.13 | SNMP TaRGETPARAMS ......................................................................................... 296 |
| 10.14 | SNMP USER ........................................................................................................... 297 |
| 10.15 | SNMP NOTIFY ....................................................................................................... 298 |
| 10.16 | SNMP FILTERPROFILE .......................................................................................... 299 |
| 10.17 | SNMP-SERVER ENABLE TRAPS SNMP AUTHENTICATION .................................... 300 |
| 10.18 | SNMP-SERVER TRAP UDP-PORT ........................................................................... 301 |
| 10.19 | SNMP-SERVER TRAP PROXY-UDP-PORT .............................................................. 302 |
| 10.20 | SNMP AGENT PORT .............................................................................................. 303 |
11.24 SHOW LOGGING-SERVER ................................................................. 378
11.25 SHOW MAIL-SERVER ................................................................. 379
11.26 SHOW SYSLOG RELAY-PORT ......................................................... 380
11.27 SHOW SYSLOG PROFILE ............................................................... 381
11.28 SHOW SYSLOG RELAY TRANSPORT TYPE ...................................... 382
11.29 SHOW SYSLOG FILE-NAME ............................................................ 383
11.30 SHOW SYSLOG INFORMATION ....................................................... 384
11.31 SMTP AUTHENTICATION ............................................................... 385
11.32 SNMP TRAP SYSLOG-SERVER-STATUS .......................................... 386

CHAPTER 12: TCP ................................................................................. 387
12.1 SHOW TCP STATISTICS ................................................................. 388
12.2 SHOW TCP CONNECTIONS ............................................................. 392
12.3 SHOW TCP LISTENERS ................................................................. 396
12.4 SHOW TCP RETRANSMISSION DETAILS .......................................... 398
12.5 TCP MAX RETRIES ................................................................. 400

CHAPTER 13: UDP ................................................................................. 401
13.1 SHOW UDP STATISTICS ................................................................. 402
13.2 SHOW UDP CONNECTIONS ............................................................. 404

CHAPTER 14: L2 DHCP SNOOPING ......................................................... 405
14.1 IP DHCP SNOOPING - GLOBAL COMMAND .................................. 406
14.2 IP DHCP SNOOPING VERIFY MAC-ADDRESS ................................ 407
14.3 IP DHCP SNOOPING - VLAN INTERFACE COMMAND .............. 408
14.4 IP DHCP SNOOPING TRUST .......................................................... 409
14.5 SHOW IP DHCP SNOOPING GLOBALS ........................................... 410
14.6 SHOW IP DHCP SNOOPING VLAN ................................................. 411
14.7 DEBUG IP DHCP SNOOPING ......................................................... 412

CHAPTER 15: IPDB ................................................................................. 413
15.1 IP BINDING .................................................................................. 414
15.2 IP SOURCE BINDING ...................................................................... 416
15.3 IP VERIFY SOURCE ......................................................................... 418
15.4 SHOW IP BINDING .......................................................................... 419
15.5 SHOW IP SOURCE BINDING .......................................................... 420
15.6 SHOW IP BINDING COUNTERS ....................................................... 422
15.7 SHOW IP VERIFY SOURCE ............................................................. 423
15.8 DEBUG IP BINDING DATABASE ...................................................... 425
Figures

Figure 2-1: Command Modes Access Path

22
Chapter 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.
• Ctrl + C - Exits from the SMIS prompt.
• 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
Chapter 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 password “ADMIN”.

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 denotes 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::BBBBB 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) #**

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit method</th>
</tr>
</thead>
<tbody>
<tr>
<td>User EXEC</td>
<td>This is the initial mode to start a session.</td>
<td>Your Product&gt;</td>
<td>The logout method is used.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>The User EXEC mode command <code>enable</code> is used to enter the Privileged EXEC mode.</td>
<td>Your Product#</td>
<td>To return from the Privileged EXEC mode to User EXEC mode the <code>disable</code> command is used.</td>
</tr>
<tr>
<td>Global Configuration</td>
<td>The Privileged EXEC mode command <code>configure terminal</code> is used to enter the Global Configuration mode</td>
<td>Your Product (config)#</td>
<td>To exit to the Privileged EXEC mode the <code>end</code> command is used.</td>
</tr>
<tr>
<td>Interface Configuration</td>
<td>The Global Configuration mode command <code>interface &lt;interface-type&gt;&lt;interface-id&gt;</code> is used to enter the</td>
<td>Your Product (config-if)#</td>
<td>To exit to the Global Configuration mode the <code>exit</code> command is used and to exit to the Privileged EXEC mode the <code>end</code> command is used.</td>
</tr>
<tr>
<td>Command Mode</td>
<td>Access Method</td>
<td>Prompt</td>
<td>Exit method</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------</td>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Interface configuration mode</td>
<td></td>
<td>Your Product(config-if-range)# Or Your Product(config-if-range)#</td>
<td>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.</td>
</tr>
<tr>
<td>Interface Range Mode</td>
<td></td>
<td>Your Product(config-if-range)# Or Your Product(config-if-range)#</td>
<td>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.</td>
</tr>
<tr>
<td>Config-VLAN</td>
<td></td>
<td>Your Product(config-vlan)#</td>
<td>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.</td>
</tr>
<tr>
<td>Line Configuration</td>
<td></td>
<td>Your Product(config-line)#</td>
<td>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.</td>
</tr>
</tbody>
</table>
2.2.1 **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.

2.2.2 **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.

2.2.3 **Global Configuration Mode**

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

2.2.4 **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.

2.2.5 **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.

2.2.5.1 **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.

2.2.5.2 **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.

2.2.5.3 **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.
2.2.6 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 the `end` command is used.

2.2.7 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.

2.2.8 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.

2.2.9 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
2.2.9.1 **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.

2.2.9.2 **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.

2.2.9.3 **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.

2.2.9.4 **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.

2.2.9.5 **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.

2.2.9.6 **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.
2.2.9.7 **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.

2.2.9.8 **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.

2.2.9.9 **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.

2.2.9.10 **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.
CHAPTER : COMMAND LINE INTERFACE

User EXEC Mode
Prompt: SMIS> enable

Privilege EXEC Mode
Prompt: SMIS#

Global Configuration Mode
Prompt: SMIS(config)#

Protocol Specific Modes
- VRRP Router Configuration
  Prompt: SMIS(config-
- VRRP Interface Configuration
  Prompt: SMIS(config-vrrp-
- DHCP Pool Configuration
  Prompt: SMIS(dhcp-config)#

General Configuration Modes
- Line Configuration
  Prompt: SMIS(config-line)#
- Interface Configuration Mode
  Prompt: SMIS(config-if)#
- Config-VLAN
  Prompt: SMIS(config-vlan)#

SNTP Configuration Mode
Prompt: SMIS(config sntp)#

Figure 2-1: Command Modes Access Pa
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
3.1 **help**

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays a brief description for the given command.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To display help description for commands with more than one word, do not provide any space between the words.</td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
<td>help [ command ]</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>All Modes</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product# help enable</td>
</tr>
<tr>
<td></td>
<td><strong>Configure Terminal command must be executed as</strong></td>
</tr>
<tr>
<td></td>
<td>Your Product# help configureterminal</td>
</tr>
</tbody>
</table>
### 3.2 clear screen

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command clears all the contents from the screen.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>clear screen</td>
</tr>
<tr>
<td>Mode</td>
<td>All Modes</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# clear screen</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>enable [0-15] Enable Level</th>
</tr>
</thead>
</table>

| Parameter Description | 0-15 Enable level - Sets the privilege 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. |

<table>
<thead>
<tr>
<th>Mode</th>
<th>User EXEC Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Enable level - 15</td>
</tr>
</tbody>
</table>

| Example | Your Product# enable 15 |

<table>
<thead>
<tr>
<th>Related Command(s)</th>
<th>disable - Turns off privileged commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable password - Modifies enable password parameters</td>
<td></td>
</tr>
</tbody>
</table>
### 3.4 disable

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>disable [&lt;0-15&gt; Privilege level to go to]</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>User EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product# disable 1</code></td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>- <code>enable</code> – Enters to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### 3.5 configure terminal

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command enters to Global Configuration Mode which allows the user to execute all the commands that supports global configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Your Product (config)#</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>- <a href="#">end</a> — Exits from Configuration mode and enters Privilidged Configuration mode</td>
</tr>
<tr>
<td></td>
<td>- <a href="#">exit</a> — Exits the current mode and reverts to the mode used prior to the current mode</td>
</tr>
</tbody>
</table>
3.6 configure

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command enters the configuration mode. Configuration from memory or network is not supported, when entered into the configuration mode using this command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>configure</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td><code>Your Product# configure</code></td>
</tr>
</tbody>
</table>
| Related Command(s)| • `end` - Exits from Current mode and enters Privileged 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** n |
| * flash: | Specifies the source of the script file. n |
| * slot0: | The script file is read from the Flash memory. n |
| * volatile: | The script file is read from the PCMCIA card or CompactFlash memory. n |
| * volatile | This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported. n |
| * <script file> | Specifies the script file to be executed n |
| * <output file> | Specifies the output file n |

**Mode**  
Privileged EXEC Mode.

**Example**  
Your Product# run script flash sample.js
### 3.8 listuser

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command lists all the default and newly created users, along with their permissible mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>listuser</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# listuser</td>
</tr>
<tr>
<td></td>
<td>USER MODE</td>
</tr>
<tr>
<td></td>
<td>ADMIN /</td>
</tr>
<tr>
<td></td>
<td>guest /</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>• show users – Displays information about terminal lines</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>lock</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# lock</td>
</tr>
</tbody>
</table>
### 3.10 username

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
</table>

#### Syntax

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

#### Parameter Description

- `<user-name>` - Specifies the login user name to be created
- `<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 maximum of 20 characters containing at least one uppercase, one lowercase, one number and one special character. The password encryption options are:
  - `privilege <1-15>` - Applies restriction to the user for accessing the CLI commands. This value 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.

#### 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.
```

#### 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 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 privileged EXEC mode
• `lisuser` - Lists all the users
### 3.11 enable password

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command modifies enable password parameters.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The no form of the command disables enable password parameters.</td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
<td><code>enable password [level (1-15)] &lt;LINE 'enable' password&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>no enable password [level (1-15)]</code></td>
</tr>
<tr>
<td><strong>Parameter Description</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>level(1-15)</code> - Represents the privilege level for which the password is to be set. The level ranges from 1 to 15.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;LINE 'enable' password&gt;</code> - Represents the password to be given. Password should follow password configuration conventions where it should contain at least one uppercase, one lowercase, one number and one special character.</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product (config)# enable password level 1 Ad@123</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>username</code> - Creates a user and sets the password for that user with the privilege level</td>
</tr>
<tr>
<td></td>
<td>• <code>enable</code> - Enters to privileged EXEC mode</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command replaces the given token by the given string. The no form of the command removes the alias created for the given string.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>alias &lt;replacement string&gt; &lt;token to be replaced&gt;</td>
</tr>
<tr>
<td></td>
<td>no alias &lt;alias&gt;</td>
</tr>
<tr>
<td>Parameter</td>
<td>&lt;replacement string&gt;/ &lt;alias&gt; - Specifies the string for which a replacement is needed.</td>
</tr>
<tr>
<td>Description</td>
<td>&lt;token to be replaced&gt; - Specifies an abbreviated/ short form of the replacement string</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# alias products pdt</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>* show aliases - Displays the aliases</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command removes the limit on number of unicast MAC entries indications to control.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`access-list provision mode { consolidated</td>
</tr>
<tr>
<td><strong>Parameter</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>consolidated</td>
<td>Configurates the provision mode as consolidated.</td>
</tr>
<tr>
<td>immediate</td>
<td>Configurates the provision mode as immediate.</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>immediate</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product (config)# access-list provision mode consolidated</code></td>
</tr>
</tbody>
</table>
3.16 access-list commit

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>access-list commit</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# access-list commit</td>
</tr>
</tbody>
</table>
3.17 `exec-timeout`

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>exec-timeout &lt;integer (1-18000)&gt;</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Line Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td>integer - 1800 seconds</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config-line)# exec-timeout 100</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>* line – Configures a console/virtual terminal line</td>
</tr>
</tbody>
</table>
## 3.18 logout

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>logout</td>
</tr>
<tr>
<td>Mode</td>
<td>User EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# logout</td>
</tr>
<tr>
<td></td>
<td>Your Product login:</td>
</tr>
</tbody>
</table>
### 3.19 end

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command exits from the current mode to the Privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>All modes</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product# end</code></td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>- <code>exit</code> - Exits the current mode and reverts to the mode used prior to the current mode.</td>
</tr>
</tbody>
</table>
### 3.20 Exit

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command exits the current mode and reverts to the mode used prior to the current mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>exit</code></td>
</tr>
<tr>
<td>Mode</td>
<td>All modes</td>
</tr>
<tr>
<td>Example</td>
<td><code>Your Product# exit</code></td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>* <code>end</code> – Exits from Configuration mode to the Privileged EXEC mode</td>
</tr>
</tbody>
</table>
### 3.21 show privilege

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command shows the current user privilege level.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show privilege</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td><code>Your Product# show privilege</code></td>
</tr>
<tr>
<td></td>
<td><code>Current privilege level is 15</code></td>
</tr>
</tbody>
</table>

**Related Command(s)**
- `enable` – Enters to Privileged EXEC Mode.
### 3.22 show line

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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays all the aliases.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show aliases</code></td>
</tr>
<tr>
<td>Mode</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# show aliases</td>
</tr>
<tr>
<td></td>
<td>show -&gt; sh</td>
</tr>
<tr>
<td></td>
<td>privilege -&gt; pr</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>- alias-replacement string – Replaces the given token by the given string</td>
</tr>
</tbody>
</table>
### 3.24 show users

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays the information about the current user.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show users</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product# show users</td>
</tr>
<tr>
<td></td>
<td>Line          User            Peer-Address</td>
</tr>
<tr>
<td></td>
<td>0 con          ADMIN          Local Peer</td>
</tr>
</tbody>
</table>

**Related Command(s)**  
* `listuser` – Lists all valid users, along with their permissible mode
### 3.25 show history

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays a list of recently executed commands.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show history</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# show history</td>
</tr>
<tr>
<td></td>
<td>1  show ip int</td>
</tr>
<tr>
<td></td>
<td>2  show debug-logging</td>
</tr>
<tr>
<td></td>
<td>3  show users</td>
</tr>
<tr>
<td></td>
<td>4  show line</td>
</tr>
<tr>
<td></td>
<td>5  show line console</td>
</tr>
<tr>
<td></td>
<td>6  c s</td>
</tr>
<tr>
<td></td>
<td>7  show aliases</td>
</tr>
<tr>
<td></td>
<td>8  show privilege</td>
</tr>
<tr>
<td></td>
<td>9  listuser</td>
</tr>
<tr>
<td></td>
<td>10 show users</td>
</tr>
<tr>
<td></td>
<td>11 show history</td>
</tr>
</tbody>
</table>
### 3.26 password validate char

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command configure the type of characters to be considered for password validation rules and takes values as bit mask.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>password validate char [lowercase] [uppercase] [numbers] [symbols]</code></td>
</tr>
<tr>
<td>Parameter Description</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>lowercase</code> - Sets lowercase flag for password validation.</td>
</tr>
<tr>
<td></td>
<td>• <code>uppercase</code> - Sets uppercase flag for password validation.</td>
</tr>
<tr>
<td></td>
<td>• <code>numbers</code> - Sets numbers flag for password validation.</td>
</tr>
<tr>
<td></td>
<td>• <code>symbols</code> - Sets symbols flag for password validation.</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td>All flags are enabled</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config)# password validate char lowercase</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>• <code>show password validate rules</code> - Displays the password validation rules.</td>
</tr>
</tbody>
</table>
3.27 `password validate uppercase`

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>password validate uppercase [&lt;count(0-20)&gt;]</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Default Value</td>
<td>1</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config) # password validate uppercase 1</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>* <a href="#">show password validate rules</a> - Displays the password validation rules.</td>
</tr>
</tbody>
</table>
### 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**

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>password validate numbers [count(0-20)]</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Default Value</td>
<td>1</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config) # password validate numbers 1</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>* show password validate rules - Displays the password validation rules.</td>
</tr>
</tbody>
</table>
### 3.30 password validate symbols

**Command Objective**
This command configures the minimum special character 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.

**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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command configures minimum password length. If the given password has less than the configured password length, it will not be allowed. This value ranges between 8 and 20.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>set minimum password length &lt;minimum-len&gt;</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td>8</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config) # set minimum password length 8</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>* show minimum password length - Displays minimum password length</td>
</tr>
</tbody>
</table>
### 3.32 show password validate rules

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the password validation rules.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show password validate rules</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td><code>Your Product# show password validate rules</code></td>
</tr>
<tr>
<td></td>
<td>Password Validation Mask : a</td>
</tr>
<tr>
<td></td>
<td>Min Lowercase char count : 2</td>
</tr>
<tr>
<td></td>
<td>Min Uppercase char count : 2</td>
</tr>
<tr>
<td></td>
<td>Min Numeric char count : 2</td>
</tr>
<tr>
<td></td>
<td>Min Symbol char count : 2</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays minimum password length.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show minimum password length</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td><code>Your Product# show minimum password length</code></td>
</tr>
<tr>
<td></td>
<td>Minimum Password length : 8</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays the password expiry time.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show password max-life-time</code></td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product# show password max-life-time</td>
</tr>
<tr>
<td></td>
<td>Password Max Life Time: 365</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>• password max-life-time - Configures the max life time after which the password has to be expired</td>
</tr>
</tbody>
</table>
Chapter 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
CHAPTER : SYSTEM FEATURES

- show nvram
- 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
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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>default restore-file &lt;filename&gt;</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td><code>smis.conf</code></td>
</tr>
<tr>
<td>Example</td>
<td><code>Your Product(config)# default restore-file restore.conf</code></td>
</tr>
<tr>
<td>Related Command(s)</td>
<td><code>show nvram</code> - Displays the current information stored in the NVRAM</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>switchport</code></td>
</tr>
<tr>
<td>no switchport</td>
<td>The interface should be shutdown before executing this command.</td>
</tr>
<tr>
<td>Mode</td>
<td>Interface Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td><code>switchport</code></td>
</tr>
<tr>
<td></td>
<td>The interface should be shutdown before executing this command.</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product(config-if)# switchport</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp</td>
<td>Allows the client device to obtain configuration parameters such as network address, from the DHCP server.</td>
</tr>
<tr>
<td>rarp</td>
<td>Allows the client device to dynamically find its IP address from RARP server, when it has only its hardware address such as MAC address.</td>
</tr>
<tr>
<td>client-id</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- GigabitEthernet - A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</td>
</tr>
<tr>
<td></td>
<td>- Port-channel - Logical interface that represents an aggregator which contains several ports aggregated together.</td>
</tr>
<tr>
<td></td>
<td>- Vlan - Logical interface that specifies a group of hosts which can communicate with each other as in same broadcast domain.</td>
</tr>
<tr>
<td>&lt;interface_list&gt;</td>
<td>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 list of interfaces. Example: 0/1,0/3 or 1,3. Feature not supported - This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.</td>
</tr>
<tr>
<td>hostname</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Mode
Interface Configuration Mode (VLAN)
CHAPTER : SYSTEM FEATURES

<table>
<thead>
<tr>
<th>Default</th>
<th>dhcp</th>
</tr>
</thead>
</table>

| 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 <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 up to 40 Gigabits per second.
    - `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-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 commas as 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 specific 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

<table>
<thead>
<tr>
<th>Mode</th>
<th>Global Configuration Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>All services are allowed for the configured manager</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config)# authorized-manager ip-source 10.203.113.5 255.255.255.255 interface gigabitethernet 0/1 vlan 1 service snmp</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>* show authorized managers - Displays the configured authorized managers</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command enables/disables HTTP in the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>set ip http {enable</td>
</tr>
<tr>
<td>Parameter Description</td>
<td>• enable - Enables HTTP in the switch.</td>
</tr>
<tr>
<td></td>
<td>• disable - Disables HTTP in the switch.</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td>enable</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product(config)# set ip http disable</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>• ip http port - Sets the HTTP port</td>
</tr>
<tr>
<td></td>
<td>• show http server status - Displays the http server status</td>
</tr>
</tbody>
</table>
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 the interface, 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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command configures the bridge port type for an interface. It is not supported but reserved for future release.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>bridge port-type { providerNetworkPort</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>providerNetworkPort</td>
<td>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.</td>
</tr>
<tr>
<td>customerNetworkPort</td>
<td>Sets the bridge port type as customer network port. It has the following options:</td>
</tr>
<tr>
<td></td>
<td>port-based – Sets the bridge port type as port based.</td>
</tr>
<tr>
<td></td>
<td>s-tagged – Sets the bridge port type as s-tagged</td>
</tr>
<tr>
<td></td>
<td>c-tagged – Sets the bridge port type as c-tagged</td>
</tr>
<tr>
<td>customerEdgePort</td>
<td>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).</td>
</tr>
<tr>
<td>propCustomerEdgePort</td>
<td>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.</td>
</tr>
<tr>
<td>propCustomerNetworkPort</td>
<td>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.</td>
</tr>
<tr>
<td>propProviderNetworkPort</td>
<td>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.</td>
</tr>
<tr>
<td>customerBridgePort</td>
<td>Sets bridge port type as Customer Bridge Port.</td>
</tr>
</tbody>
</table>
CHAPTER : SYSTEM FEATURES

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.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Interface Configuration Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>providerNetworkPort for provider core and edge bridges.</td>
</tr>
<tr>
<td></td>
<td>customerBridgePort for customer bridges.</td>
</tr>
</tbody>
</table>

- 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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command configures the custom parameters for a particular port. The no form of the command deletes the custom parameter configurations.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td>`set custom-param {type &lt;integer&gt; length &lt;integer&gt; value &lt;string&gt;</td>
</tr>
<tr>
<td></td>
<td><code>no custom-param [type &lt;integer&gt;] [attribute &lt;integer (1-4)&gt;]</code></td>
</tr>
<tr>
<td><strong>Parameter Description</strong></td>
<td></td>
</tr>
<tr>
<td>• <strong>type</strong> -</td>
<td>Sets the type of the TLV information.</td>
</tr>
<tr>
<td>• <strong>length</strong> -</td>
<td>Sets the length of the TLV information.</td>
</tr>
<tr>
<td>• <strong>value</strong> -</td>
<td>Sets the value of the TLV information.</td>
</tr>
<tr>
<td>• <strong>attribute</strong> -</td>
<td>Sets the opaque attribute ID configured on the port. The value ranges between 1 and 4.</td>
</tr>
<tr>
<td>• <strong>value</strong> -</td>
<td>Sets the value for the Opaque attribute. The value ranges between 0 and 4294967295.</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Interface Configuration Mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>value - 0</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product(config-if)# set custom-param attribute 2 value 40</code></td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td></td>
</tr>
</tbody>
</table>
4.16 mac-addr

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command configures unicast MAC address for the interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>mac-addr <a href="">aa:aa:aa:aa:aa:aa</a></td>
</tr>
<tr>
<td>Mode</td>
<td>Interface Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td>MAC address of the switch is assigned as MAC address for the interface.</td>
</tr>
</tbody>
</table>

- 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`

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>snmp trap link-status</code></td>
</tr>
<tr>
<td></td>
<td><code>no snmp trap link-status</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Interface Configuration Mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>SNMP trap link status is enabled</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product(config-if)# snmp trap link-status</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>* <code>show interfaces</code> - Displays the interface status and configuration.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command copies the configuration from a remote site to flash.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`copy { tftp://ip-address/filename startup-config</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td>• <code>tftp://ip-address/ filename startup-config</code> - 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</td>
</tr>
<tr>
<td></td>
<td>• <code>sftp://&lt;user-name&gt;:&lt;pass-word&gt;@ip-address/ filename</code> - Configures the name of the file in remote location to be copied (downloaded) into configuration file (smis.conf). This option configures the SFTP server details. Filenames and directory names are case sensitive</td>
</tr>
<tr>
<td></td>
<td>• <code>flash: filename startup-config</code> - Configures the name of the file in flash. The configuration in the flash file are used. Filenames are case sensitive</td>
</tr>
<tr>
<td></td>
<td>• <code>cust:/filename startup-config</code> - Configures the name of the file in USB drive. The configuration in the USB flash file are used. Filenames are case sensitive</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td><code>Your Product# copy flash:clcliser startup-config</code></td>
</tr>
</tbody>
</table>
CHAPTER : SYSTEM FEATURES

4.20 copy startup-config

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

**Syntax**

```plaintext
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**

```plaintext
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 system logs to a remote site.

Syntax:

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

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}
```

<table>
<thead>
<tr>
<th>Parameter Description</th>
<th>Description</th>
</tr>
</thead>
</table>
| `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

**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**
```plaintext
copy {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 Mode

**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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command manages the system clock.</th>
</tr>
</thead>
</table>

### 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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command clears the contents of the startup configuration or sets parameters in NVRAM to default values.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>erase {startup-config</td>
</tr>
<tr>
<td>Parameter Description</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• startup-config - Clears the startup configuration file</td>
</tr>
<tr>
<td></td>
<td>• nvram - Clears the content from NVRAM</td>
</tr>
<tr>
<td></td>
<td>• flash:filename - Clears the content from the local system flash file.</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# erase startup-config</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• show nvram - Displays the current information stored in the NVRAM</td>
</tr>
<tr>
<td></td>
<td>• show system information - Displays system information</td>
</tr>
</tbody>
</table>
### 4.27 cli console

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command enables the console CLI through a serial port. The no form of the command disables console CLI.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>cli console</code></td>
</tr>
<tr>
<td></td>
<td><code>no cli console</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>This command takes effect only on system restart.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product# cli console</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td><code>show nvram</code> - Displays the current information stored in the NVRAM.</td>
</tr>
</tbody>
</table>
### 4.28 flowcontrol

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command is used to set the send or receive flow-control value for an interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Parameter Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>send</td>
<td>Sets the interface to send flow control packets to a remote device</td>
</tr>
<tr>
<td>receive</td>
<td>Sets the interface to receive flow control packets from a remote device</td>
</tr>
<tr>
<td>on</td>
<td>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</td>
</tr>
<tr>
<td>off</td>
<td>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</td>
</tr>
<tr>
<td>desired</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mode</th>
<th>Interface Configuration Mode</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>The default flow control for the interfaces are</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• flowcontrol receive off</td>
</tr>
<tr>
<td></td>
<td>• flowcontrol send off</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th><code>Your Product(config-if)# flowcontrol send on</code></th>
</tr>
</thead>
</table>
### 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

**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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>tunnel checksum</code></td>
</tr>
<tr>
<td></td>
<td><code>no tunnel checksum</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Interface Configuration Mode (Tunnel interface mode)</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>disabled</td>
</tr>
</tbody>
</table>

*This command is applicable only for GRE Encapsulation Method.*

**Example**

```bash
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`

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command associates tunnel with a unidirectional interface. It is not supported. The no form of the command associates tunnel with a Bidirectional interface.</th>
</tr>
</thead>
</table>
| 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**
```
depth 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 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 buffer or to a file, which can later be uploaded, based on the input.

The no form of the command displays debug logs in the console.

**Syntax**
```
debug-logging { console | file | flash}
no debug-logging
```

**Parameter Description**
- **console** - Specifies the logging of traces at the console
- **file** - Specifies the logging of traces to a system buffer/memory
- **flash** - Specifies the logging of traces into a file

**Mode**  Global Configuration Mode

**Default**  console

**Example**
```
Your Product(config)# debug-logging console
```

**Related Command(s)**
- **show debug-logging** - Displays the debug logs stored in file
# 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

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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
</table>

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

Utility: Power

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.

Syntax
```
set switch power {min|max} threshold <volts (100-230)>
```

Parameter Description
- **min** - Sets the minimum threshold power supply for the switch. When the voltage drops below the threshold, an SNMP trap with maximum severity will be sent to the manager.
- **max** - Sets the maximum threshold power supply 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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command sets the system location.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>system location &lt;location name&gt;</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product(config)# system location Controls</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td><code>show system information</code> - Displays system information.</td>
</tr>
</tbody>
</table>
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.
  - `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: `0/1` represents 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 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: 0/1 represents 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: 0/1 represents 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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the interface status and configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>show interfaces {{ [ [&lt;interface-type&gt; &lt;interface-id&gt;]] [description</td>
</tr>
<tr>
<td>Parameter Description</td>
<td></td>
</tr>
<tr>
<td>• &lt;interface-type&gt;</td>
<td>Displays the interface status and configuration for the specified type of interface. The interface can be:</td>
</tr>
<tr>
<td></td>
<td>− qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.</td>
</tr>
<tr>
<td></td>
<td>− gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</td>
</tr>
<tr>
<td></td>
<td>− extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</td>
</tr>
<tr>
<td>• &lt;interface-id&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>• Description</td>
<td>Displays the interface description.</td>
</tr>
<tr>
<td>• storm-control</td>
<td>Displays the broadcast, multicast, and unicast storm control suppression levels for the specified interface</td>
</tr>
<tr>
<td>• flowcontrol</td>
<td>Displays the flow control related statistics information for the specified interface.</td>
</tr>
<tr>
<td>• capabilities</td>
<td>Displays the interface type, interface speed, duplex operation and flowcontrol status for the specified interface.</td>
</tr>
<tr>
<td>• status</td>
<td>Displays the status, duplex details, speed and negotiation mode of the specified interface.</td>
</tr>
<tr>
<td>• port-security-state</td>
<td>Displays the state of the port security option.</td>
</tr>
<tr>
<td>• vlan &lt;vlan-id/vfi-id&gt;</td>
<td>Displays the interface status and configuration for the specified VLAN/ VFI ID. This value ranges between 1 and 65535.</td>
</tr>
</tbody>
</table>
| | − <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<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

<table>
<thead>
<tr>
<th>Example</th>
<th>Privileged EXEC Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your product# show interfaces gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td>Gi0/1 up, line protocol is up (connected)</td>
<td></td>
</tr>
<tr>
<td>Bridge Port Type: Customer Bridge Port</td>
<td></td>
</tr>
<tr>
<td>Hardware Address is 00:01:02:03:04:22</td>
<td></td>
</tr>
<tr>
<td>RARP Client is enabled</td>
<td></td>
</tr>
<tr>
<td>MTU 1500 bytes, Full duplex, 100 Mbps, Auto-Negotiation</td>
<td></td>
</tr>
<tr>
<td>HOL Block Prevention enabled.</td>
<td></td>
</tr>
<tr>
<td>Invalid flowcontrol Mode</td>
<td></td>
</tr>
<tr>
<td>Link Up/Down Trap is enabled</td>
<td></td>
</tr>
<tr>
<td>Reception Counters</td>
<td></td>
</tr>
<tr>
<td>Octets : 0</td>
<td></td>
</tr>
<tr>
<td>Unicast Packets : 0</td>
<td></td>
</tr>
<tr>
<td>Discarded Packets : 0</td>
<td></td>
</tr>
</tbody>
</table>
Error Packets            : 0  
Unknown Protocol         : 0  
Transmission Counters 
Octets                   : 8266  
Unicast Packets          : 0  
Discarded Packets        : 0  
Error Packets            : 0  

Your product# show interfaces description 
<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>Protocol Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Gi0/2</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>vlan1</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>acl</td>
<td>down</td>
<td>down</td>
</tr>
</tbody>
</table>

Your product# show interfaces gigabitethernet 0/2 storm control 
Gi0/2
  DLF Storm Control            : Disabled 
  DLF Storm Control Limit      : 0  
  Broadcast Storm Control      : Enabled 
  Broadcast Storm Control      : 0  
  Multicast Storm Control      : Enabled 
  Multicast Storm Control      : 0  

Your product# show interfaces gigabitethernet 0/2 flow-control 
Port Tx FlowControl Rx FlowControl Tx Pause Rx Pause HC 
--- -------------- ------------- -------- -------- ------ 
Gi0/2 off     off           0       0      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 
--- -------------- ------------- -------- --------
CHAPTER : SYSTEM FEATURES

---       ---     ---       ---     ---     ---
G10/2  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 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 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 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 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.

### Example

<table>
<thead>
<tr>
<th>Mode</th>
<th>Privileged EXEC Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example</strong></td>
<td><strong>Your Product# show interfaces counters</strong></td>
</tr>
<tr>
<td></td>
<td>Port InOctet InUcast InDiscard InErrs InHCOctet</td>
</tr>
<tr>
<td>Gi0/1</td>
<td>115043 1380 690 0 115043</td>
</tr>
<tr>
<td>vlan1</td>
<td>0 0 0 0 0</td>
</tr>
<tr>
<td>vlan10</td>
<td>0 0 0 0 0</td>
</tr>
<tr>
<td>Port OutOctet</td>
<td>OutUcast OutDiscard OutErrs OutHCOctet</td>
</tr>
<tr>
<td>Gi0/1</td>
<td>12145 0 0 0 12145</td>
</tr>
<tr>
<td>vlan1</td>
<td>120 1 0 0 120</td>
</tr>
<tr>
<td>vlan10</td>
<td>0 0 0 0 0</td>
</tr>
<tr>
<td><strong>Your Product# show interfaces counters vlan 10</strong></td>
<td></td>
</tr>
<tr>
<td>Port InOctet</td>
<td>InUcast InDiscard InErrs InHCOctet</td>
</tr>
<tr>
<td>----</td>
<td>------- ------- ------- -------</td>
</tr>
<tr>
<td>vlan10</td>
<td>0 0 0 0</td>
</tr>
<tr>
<td>Port OutOctet</td>
<td>OutUcast OutDiscard OutErrs OutHCOctet</td>
</tr>
<tr>
<td>----</td>
<td>------- ------- ------- -------</td>
</tr>
<tr>
<td>vlan10</td>
<td>0 0 0 0</td>
</tr>
</tbody>
</table>
### System Features

#### Command Output

Your Product # show interfaces HC counters

<table>
<thead>
<tr>
<th>Port</th>
<th>InHCOctet</th>
<th>InUcastPkts</th>
<th>InMulticastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1</td>
<td>129886</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>vlan1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>vlan10</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>OutHCOctet</th>
<th>OutUcastPkts</th>
<th>OutMulticastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1</td>
<td>14071</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>vlan1</td>
<td>120</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>vlan10</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Your Product# show interfaces HC counters gi 0/1

<table>
<thead>
<tr>
<th>Port</th>
<th>InHCOctet</th>
<th>InUcastPkts</th>
<th>InMulticastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1</td>
<td>153868</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>OutHCOctet</th>
<th>OutUcastPkts</th>
<th>OutMulticastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1</td>
<td>16730</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Interface PortID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot0/1 45</td>
</tr>
</tbody>
</table>

**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 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.
  - 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 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.

- `<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 that the slot number is 0 and port number is 1.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Privileged EXEC Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td><code>Your product# show interface mtu Vlan 1</code></td>
</tr>
<tr>
<td></td>
<td><code>vlan1   MTU size is 1500</code></td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>• <code>mtu</code> Configures the maximum transmission unit frame size for the interface</td>
</tr>
</tbody>
</table>
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 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.
- **<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 is 100. This interface type is not supported.

**Mode**
Privileged EXEC Mode

**Example**
```
Your product# show interface bridge port-type
Gi0/1 Bridge port type is Customer Bridge Port
Gi0/2 Bridge port type is Customer Bridge Port
Gi0/3 Bridge port type is Customer Bridge Port
Gi0/4 Bridge port type is Customer Bridge Port
Gi0/5 Bridge port type is Customer Bridge Port
Gi0/6 Bridge port type is Customer Bridge Port
Gi0/7 Bridge port type is Customer Bridge Port
Gi0/8 Bridge port type is Customer Bridge Port
```
Gi0/9 Bridge port type is Customer Bridge Port
Gi0/10 Bridge port type is Customer Bridge Port
Gi0/11 Bridge port type is Customer Bridge Port
Gi0/12 Bridge port type is Customer Bridge Port
Gi0/13 Bridge port type is Customer Bridge Port
Gi0/14 Bridge port type is Customer Bridge Port
Gi0/15 Bridge port type is Customer Bridge Port
Gi0/16 Bridge port type is Customer Bridge Port
Gi0/17 Bridge port type is Customer Bridge Port
Gi0/18 Bridge port type is Customer Bridge Port
Gi0/19 Bridge port type is Customer Bridge Port
Gi0/20 Bridge port type is Customer Bridge Port
Gi0/21 Bridge port type is Customer Bridge Port
Gi0/22 Bridge port type is Customer Bridge Port
Gi0/23 Bridge port type is Customer Bridge Port
Gi0/24 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
```


<table>
<thead>
<tr>
<th>Firmware Version</th>
<th>2.0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Part Number</td>
<td>MBM-XEM-002</td>
</tr>
<tr>
<td>Software Serial Number</td>
<td>1-0-0</td>
</tr>
<tr>
<td>Software Version</td>
<td>6.12.0</td>
</tr>
<tr>
<td>Switch Name</td>
<td>SMIS</td>
</tr>
<tr>
<td>RM Heart Beat Mode</td>
<td>Internal</td>
</tr>
<tr>
<td>RM Redundancy Type</td>
<td>Hot</td>
</tr>
<tr>
<td>RM Data Plane Type</td>
<td>Shared</td>
</tr>
<tr>
<td>RM Type</td>
<td>OOB</td>
</tr>
<tr>
<td>NPAPI mode</td>
<td>Synchronous</td>
</tr>
<tr>
<td>TimeStamp Method</td>
<td>Software</td>
</tr>
<tr>
<td>Restore Flag</td>
<td>Disabled</td>
</tr>
<tr>
<td>Dynamic Port Count</td>
<td>64</td>
</tr>
<tr>
<td>FIPS operation mode</td>
<td>Disabled</td>
</tr>
<tr>
<td>Restore Option</td>
<td>Disabled</td>
</tr>
<tr>
<td>Bridge Mode</td>
<td>Customer Bridge</td>
</tr>
<tr>
<td>Management Port</td>
<td>Disabled</td>
</tr>
<tr>
<td>Automatic Port Create Flag</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**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 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 Celsius
- **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 supply 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 Environment Values

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Temperature</td>
<td>40°C</td>
</tr>
<tr>
<td>Flash Threshold</td>
<td>90%</td>
</tr>
<tr>
<td>Current Flash Threshold</td>
<td>62%</td>
</tr>
<tr>
<td>Mgmt Port Routing</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**Your product# show env RAM**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM Threshold</td>
<td>98%</td>
</tr>
<tr>
<td>Current RAM Threshold</td>
<td>97%</td>
</tr>
</tbody>
</table>

**Your product# show env power**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min power supply</td>
<td>110v</td>
</tr>
<tr>
<td>Max power supply</td>
<td>220v</td>
</tr>
<tr>
<td>Current power supply</td>
<td>230v</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays system information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>show system information</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your product# show system information</td>
</tr>
<tr>
<td></td>
<td>Hardware Version : 1.0.1</td>
</tr>
<tr>
<td></td>
<td>Firmware Version : 2.0.0</td>
</tr>
<tr>
<td></td>
<td>Hardware Part Number : MBM-XEM-002</td>
</tr>
<tr>
<td></td>
<td>Software Serial Number : 1-0-0</td>
</tr>
<tr>
<td></td>
<td>Software Version : 2.0.0</td>
</tr>
<tr>
<td></td>
<td>Switch Name : SMIS</td>
</tr>
<tr>
<td></td>
<td>System Contact : Supermicro</td>
</tr>
<tr>
<td></td>
<td>System Location : Supermicro</td>
</tr>
<tr>
<td></td>
<td>Logging Option : Console Logging</td>
</tr>
<tr>
<td></td>
<td>Login Authentication Mode : Local</td>
</tr>
<tr>
<td></td>
<td>Config Save Status : Not Initiated</td>
</tr>
<tr>
<td></td>
<td>Remote Save Status : Not Initiated</td>
</tr>
<tr>
<td></td>
<td>Config Restore Status : Not Initiated</td>
</tr>
<tr>
<td></td>
<td>Traffic Separation Control : none</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the flow-control information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show flow-control [ interface &lt;interface-type&gt; &lt;interface-id&gt; ]</code></td>
</tr>
</tbody>
</table>
| 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 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 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: 0/1 represents 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 Tx FlowControl Rx FlowControl Tx Pause Rx Pause  
  HC TxPause HC RxPause  
  ---- ------------------ ----------------- ----  
  ---- ------------------  
  Gi0/2 on on 0 0 0 |
| Related Command(s) | • `show interfaces` - Displays interface status and configuration  
  • `flowcontrol` - Enables flowcontrol on an interface |
### 4.58 show debug-logging

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the debug logs stored in file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show debug-logging</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product(config)# debug-logging file</td>
</tr>
<tr>
<td></td>
<td>Your Product(config)# exit</td>
</tr>
<tr>
<td></td>
<td>Your product# debug spanning-tree events</td>
</tr>
<tr>
<td></td>
<td>Your product# show debug-logging</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Timer Expiry Event processed...</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Completed processing the event(s).</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Timer Expiry Event processed...</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Completed processing the event(s).</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Timer Expiry Event processed...</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Completed processing the event(s).</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Timer Expiry Event processed...</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Completed processing the event(s).</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Timer Expiry Event processed...</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Completed processing the event(s).</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Timer Expiry Event processed...</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Completed processing the event(s).</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Timer Expiry Event processed...</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Completed processing the event(s).</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Timer Expiry Event processed...</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Completed processing the event(s).</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Completed processing the event(s).</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Completed processing the event(s).</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Completed processing the event(s).</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Completed processing the event(s).</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Completed processing the event(s).</td>
</tr>
<tr>
<td></td>
<td>AST: MSG: Completed processing the event(s).</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>* debug-logging - Configures where debug logs are to be displayed</td>
</tr>
</tbody>
</table>
### 4.59 show debugging

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays state of each debugging option.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show debugging</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your product# show debugging</td>
</tr>
<tr>
<td></td>
<td>Spanning Tree :</td>
</tr>
<tr>
<td></td>
<td>Spanning tree timers related debugging is on</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td></td>
</tr>
<tr>
<td>debug spanning-tree</td>
<td>Provides spanning tree debugging support</td>
</tr>
<tr>
<td>debug dot1x</td>
<td>Enables debugging of dot1x module</td>
</tr>
<tr>
<td>debug radius</td>
<td>Enables RADIUS debugging options</td>
</tr>
<tr>
<td>debug ip igmp snooping</td>
<td>Specifies the debug levels for the IGMP snooping module</td>
</tr>
<tr>
<td>debug ssh</td>
<td>Sets the given trace levels for SSH</td>
</tr>
<tr>
<td>debug ssl</td>
<td>Sets the given debug levels for SSL</td>
</tr>
<tr>
<td>debug vlan</td>
<td>Enables the tracing of the VLAN submodule as per the configured debug levels.</td>
</tr>
<tr>
<td>debug garp</td>
<td>Enables the tracing of the GARP submodule as per the configured debug levels.</td>
</tr>
<tr>
<td>debug ip dhcp client</td>
<td>Enables the tracking of the DHCP client operations as per the configured debug levels.</td>
</tr>
<tr>
<td>debug ip dhcp relay</td>
<td>Enables the debug level for tracing the DHCP Relay Module</td>
</tr>
<tr>
<td>debug ip dhcp server</td>
<td>Enables the tracking of the DHCP server operations as per the configured debug levels.</td>
</tr>
</tbody>
</table>
### 4.60 show clock

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays the system date and time.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show clock</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your product# show clock</code></td>
</tr>
<tr>
<td></td>
<td><code>Fri Jun 28 08:31:19 2013 (UTC +05:50)</code></td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td><code>clock set</code> - Manages the system clock</td>
</tr>
</tbody>
</table>
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 | rip6 | ipv6 | ipv6 | 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 | clkifi | mld | md5 | madpv6 | lldp | firewall | system | ospfte | ipsourceguard | tlm | rbridge | l2dhsnp | mfp | network-clock | vrf <vrf-name> | bs | bfd | qosxtd | dsmon | mfp | 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.
CHAPTER: SYSTEM FEATURES

- `<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 upto 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 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 entity-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

<table>
<thead>
<tr>
<th>Mode</th>
<th>Privileged EXEC Mode</th>
</tr>
</thead>
</table>

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...
spanningtree 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
tIdentity is 100.20.6.100, autonomous system 100
bgp default ipv4-unicast
<table>
<thead>
<tr>
<th>Command(s)</th>
<th>Related Command include the configuration commands of all the modules (given as parameters in the show running-config command)</th>
</tr>
</thead>
<tbody>
<tr>
<td>redistribute static</td>
<td></td>
</tr>
<tr>
<td>restart-reason</td>
<td></td>
</tr>
<tr>
<td>softwareRestart</td>
<td></td>
</tr>
<tr>
<td>neighbor 100.20.6.20 remote as 200</td>
<td></td>
</tr>
<tr>
<td>neighbor 100.20.6.20 update-source 100.20.6.100</td>
<td></td>
</tr>
<tr>
<td>neighbor 100.20.6.20 timers holdtime 240</td>
<td></td>
</tr>
<tr>
<td>neighbor 110.20.6.20 remote-as 300</td>
<td></td>
</tr>
<tr>
<td>neighbor 110.20.6.20 update-source 110.20.6.100</td>
<td></td>
</tr>
<tr>
<td>neighbor 110.20.6.20 timers holdtime 240</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays acknowledgement statement for open sources used in the software.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show system acknowledgement</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your product# show system acknowledgement</code></td>
</tr>
</tbody>
</table>

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.radixs.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

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
```

<table>
<thead>
<tr>
<th>Ingress Port</th>
<th>VlanId</th>
<th>StorageType</th>
<th>Egress List</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/2</td>
<td>10</td>
<td>Non-Volatile</td>
<td>Gi0/1</td>
</tr>
<tr>
<td>Gi0/3</td>
<td>-</td>
<td>Non-Volatile</td>
<td>Gi0/2</td>
</tr>
</tbody>
</table>

#### 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.

```
private-vlan mapping [(add | remove)] <vlan-list>
```

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.

**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**
- `enable` - Enables audit logging.
- `disable` - Disables audit logging.

**Mode**
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 maximum file size in Kilobytes of the configs.txt file
- `audit-logging reset` - Erases the contents in configs.txt file and start logging
- `show config log` - Displays Information related to Audit Logging
## 4.69 audit-logging filename

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command specifies the name of the file to which Audit log is saved. The maximum string value of the file name is 128.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>audit-logging filename &lt;filename&gt;</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>Config.txt</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product(config)# audit-logging filename srv.txt</code></td>
</tr>
</tbody>
</table>

**Related Command(s)**

- `audit-logging` - Enables/disables audit logging
- `audit-logging filesize` - Specifies 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 config 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**  
\[
\text{audit-logging filesize} \ <\text{filesize}(1024-1048576)> 
\]

**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 config log` - Displays Information related to Audit Logging
4.71 audit-logging reset

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command is used to erase the contents in configs.txt file and start logging.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>audit-logging reset</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product(config)# audit-logging reset</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• audit-logging – Enables/disables audit logging</td>
</tr>
<tr>
<td></td>
<td>• audit-logging filesize – Specifies the the maximum file size in Kilobytes of the configs.txt file</td>
</tr>
<tr>
<td></td>
<td>• audit-logging filename – Specifies the name of the file to which Audit log is saved</td>
</tr>
<tr>
<td></td>
<td>• show config log – Displays Information related to Audit Logging</td>
</tr>
</tbody>
</table>
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 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 disable the Head-of-Line Blocking prevention which manages the HOL blocking situation by checking whether the packet has been assigned priority. If the packets have assigned priority, those packets are placed in a separate queue. The low priority data can be discarded as applications keep track of whether a retransmission is necessary or not.

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

**Syntax**  

hol blocking prevention

**Mode**  

Global 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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays the internal lan parameters.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show internal-lan &lt;iface_list&gt;</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your product# show internal-lan</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td><code>internal-lan-</code> Adds an ilan interface and its parameters</td>
</tr>
</tbody>
</table>
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.

Syntax
\texttt{clear line vty \{<line-number(2-9)> | all\}}

Parameter Description
- \texttt{<line-number(2-9)>} - Clears the vty information of the specified telnet session. This value ranges between 2 and 9.
- \texttt{all} - Clears all the vty information.

Mode
Privileged EXEC Mode

Example
Your Product\# clear line vty 2

Related Command(s)
- \texttt{show line} --- Displays the TTY line information
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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command configures the maximum number of successful login attempts and the lock out time to block the user.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>login block-for &lt;seconds(30-600)&gt; attempts &lt;tries(1-10)&gt;</code></td>
</tr>
<tr>
<td><strong>Parameter Description</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;seconds(30-600)&gt;</code> - Configures the lock out time in seconds that a user is blocked following unsuccessful logins. This value ranges between 30 and 600.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;tries(1-10)&gt;</code> - 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.</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global Configuration mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>• seconds - 3</td>
</tr>
<tr>
<td></td>
<td>• tries - 3</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product(config)# login block-for 30 attempts 3</code></td>
</tr>
</tbody>
</table>
### 4.80 audit-logging logsize-threshold

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>audit-logging logsize-threshold &lt;threshold in % (1-99)&gt;</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global Configuration mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>threshold in % - 70</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product (config)# audit-logging logsize-threshold 99</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>- <code>show config log</code> - Displays the information related to Audit Logging.</td>
</tr>
</tbody>
</table>
### 4.81 feature telnet

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command enables the telnet service in the system. The no form of this command disables the telnet service.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td>feature telnet</td>
</tr>
<tr>
<td></td>
<td>no feature telnet</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global Configuration mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>The telnet service is enabled</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product(config)# feature telnet</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>* show telnet server - Displays the telnet server status.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the content of the audit-log file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show audit</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
</tbody>
</table>

**Example**

```
Your Product# show audit
Audit:ADMIN audit logging         SUCCESS CONSOLE Fri Jun 10 reset21:27:54 2011
Audit:ADMIN firewall             SUCCESS CONSOLE Fri Jun 10 21:27:57 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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command configures the Configurable HTTP authentication scheme.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`set http authentication-scheme {default</td>
</tr>
<tr>
<td>Parameter Description</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>default</code> - Sets the configurable HTTP authentication scheme to default.</td>
</tr>
<tr>
<td></td>
<td>• <code>basic</code> - Sets the configurable HTTP authentication scheme to basic.</td>
</tr>
<tr>
<td></td>
<td>• <code>digest</code> - Sets the configurable HTTP authentication scheme to digest.</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td><code>default</code></td>
</tr>
<tr>
<td>Example</td>
<td><code>Your Product (config)# set http authentication-scheme basic</code></td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>• <code>show http authentication-scheme</code> - Displays the Operational and Configurable authentication scheme values.</td>
</tr>
</tbody>
</table>
### 4.85 set http redirection enable

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command enables the HTTP redirection feature. The no form of this command disables the HTTP redirection feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>set http redirection enable</td>
</tr>
<tr>
<td></td>
<td>no http redirection enable</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td>HTTP redirection is disabled</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config)# set http redirection enable</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays the operational and configurable authentication scheme values.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show http authentication-scheme</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product# show http authentication-scheme</code></td>
</tr>
<tr>
<td></td>
<td>The Operational HTTP authentication scheme is Digest</td>
</tr>
<tr>
<td></td>
<td>The Configured HTTP authentication scheme is Digest</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the redirection entries filtered by URL or all the entries.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show http redirection [URL]</code></td>
</tr>
<tr>
<td>Parameter</td>
<td><strong>URL</strong> - Configures the URL for which the redirection entry has to be displayed.</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td><code>Your Product# show http redirection /sample/</code></td>
</tr>
<tr>
<td></td>
<td>HTTP Redirection Entries</td>
</tr>
<tr>
<td></td>
<td>----------------------------------- -------------------------------------------</td>
</tr>
<tr>
<td>URL</td>
<td>Server IP/DomainName</td>
</tr>
<tr>
<td>/sample/</td>
<td>12.0.0.2</td>
</tr>
</tbody>
</table>

**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
4.89.1 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
### 4.89.2 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.
4.89.3 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: Supermicro
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
4.89.4 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
4.89.5 show entity alias-mapping

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>show entity alias-mapping [index &lt;integer (1..2147483647)&gt;]</td>
</tr>
<tr>
<td>Parameter</td>
<td>• index &lt;integer (1..2147483647)&gt; - Displays the Index of the physical entity. The value ranges between 1 and 2147483647.</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your product# show entity alias-mapping</td>
</tr>
<tr>
<td></td>
<td>Physical Index 10 for all Logical entities is mapped to external identifier : Gi0/1</td>
</tr>
<tr>
<td></td>
<td>Physical Index 11 for all Logical entities is mapped to external identifier : Gi0/24</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>• interface - configuration and deletion - Configures interface such as out of band management, port channel, tunnel and so on.</td>
</tr>
</tbody>
</table>
### 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 (Chassis)
  Member Physical Entities: 2 (Cpu), 3 (Power Supply), 4 (Fan)
                             5 (Fan), 6 (Fan), 7 (Fan)
                             8 (Fan), 9 (Module)
  Physical Entity         : 9 (Module)
  Member Physical Entities: 10 (Port), 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)
```

### Related Command(s)
- **interface** - configuration and deletion - Configures interface such as out of band management, port channel, tunnel and so on
4.90  set hitless-restart enable

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>set hitless-restart enable</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Default</td>
<td>Hitless restart is disabled.</td>
</tr>
</tbody>
</table>

**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
```
### 4.91 speed

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command sets the speed of the interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td>`speed { 10</td>
</tr>
<tr>
<td><strong>Parameter Description</strong></td>
<td></td>
</tr>
<tr>
<td>• 10 - Sets the port to run at 10Mbps.</td>
<td></td>
</tr>
<tr>
<td>• 100 - Sets the port to run at 100Mbps.</td>
<td></td>
</tr>
<tr>
<td>• 1000 - Sets the port to run at 1000Mbps.</td>
<td></td>
</tr>
<tr>
<td>• 10000 - Sets the port to run at 10000Mbps.</td>
<td></td>
</tr>
<tr>
<td>• 40000 - Sets the port to run at 40000Mbps.</td>
<td></td>
</tr>
<tr>
<td>• 56000 - Sets the port to run at 56000Mbps.</td>
<td></td>
</tr>
<tr>
<td>• auto - Detects and sets the speed of the port automatically based on the peer switch.</td>
<td></td>
</tr>
<tr>
<td>• nonegotiate - Disables negotiation on the ports.</td>
<td></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Interface Configuration Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product (config-if)# speed 10</td>
</tr>
</tbody>
</table>
### 4.92 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
4.93 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
```plaintext
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.
### 4.94 sleep

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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 65535 in seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>sleep &lt;seconds(1-65535)&gt;</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td><code>Your Product# sleep 51</code></td>
</tr>
</tbody>
</table>
## 4.95 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** | Your Product (config-if)# rate-limit pause 400000 300000 |
## 4.96 cpu controlled learning

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>cpu controlled learning</code></td>
</tr>
<tr>
<td></td>
<td><code>no cpu controlled learning</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Interface Configuration Mode (Physical)</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product (config-if)# cpu controlled learning</code></td>
</tr>
</tbody>
</table>
4.97 **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}

<table>
<thead>
<tr>
<th>Parameter Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System_default</td>
<td>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.</td>
</tr>
<tr>
<td>User_defined</td>
<td>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.</td>
</tr>
<tr>
<td>none</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.
### 4.98 mdix auto

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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 sets the port as MDIX port.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>mdix auto</code></td>
</tr>
<tr>
<td></td>
<td><code>no mdix auto</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Interface Configuration Mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>AutoCross is disabled</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product (config-if)# mdix auto</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>• <code>set port</code> - Sets the port to MDI or MDIX mode</td>
</tr>
</tbody>
</table>
### 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
# 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}
```

## 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. This
- **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.

## Mode
- **Privileged EXEC Mode**

## Default
- **norestore**

## Example
```
Your Product# config-restore flash
```

## Related Command(s)
- **show system information** – Displays the system information.
### 4.101 set switch-name

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command sets the name of the switch. This is a string with maximum size as 15.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>set switch-name &lt;switchname&gt;</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product(config)# set switch-name sw1</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>• show system information – Displays the system information</td>
</tr>
</tbody>
</table>
**4.102 packet receive index**

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command configures the packet pattern and mask for pattern matching on the received packets.</th>
</tr>
</thead>
</table>
| 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 which uniquely 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. |
4.103 **packet send index port**

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>packet send index &lt;integer (0-4)&gt; port &lt;port_list&gt; [count &lt;integer (0-65536)&gt; [interval &lt;integer (1-65535)&gt;]]no packet send index &lt;integer (0-4)&gt;</code></td>
</tr>
</tbody>
</table>
| Parameter Description | • `<integer (0-4)>` - Configures the packet send index value which uniquely 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. |
4.104 `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.
### 4.105 show packet send index

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the values of the packet transmitter table. The packet send index ranges between 0 and 4.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show packet send index &lt;integer(0-4)&gt;</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# show packet send index 1</td>
</tr>
<tr>
<td></td>
<td>Index : 1</td>
</tr>
<tr>
<td></td>
<td>Value of the Pkt :</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>• <code>packet send index value</code> - Sets the port, interval, count for the packet transmitter and transmits the packet provided the packet pattern is configured.</td>
</tr>
<tr>
<td></td>
<td>• <code>packet send index port</code> - Sets the packet pattern for the packet transmitter and transmits the packet, provided the interface is configured.</td>
</tr>
</tbody>
</table>
### 4.106 show packet receive index

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the values of the packet receiver table. The packet receive index ranges between 0 and 4.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>show packet receive index &lt;integer(0-4)&gt;</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# show packet receive index 1</td>
</tr>
</tbody>
</table>

**Packet Analyzer**

**Related Command(s)** packet receive index - Configures the packet pattern and mask for pattern matching on the received packets.
### 4.107 set mirroring

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command enables or disables the mirroring in the system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>set mirroring {enable</td>
</tr>
<tr>
<td>Parameter Description</td>
<td></td>
</tr>
<tr>
<td>• enable – Enables mirroring in the system. When set as enabled all mirroring configurations present will be programmed in hardware.</td>
<td></td>
</tr>
<tr>
<td>• disable – Disables mirroring in the system and removes all configuration from the hardware</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td>enable</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product(config)# set mirroring enable</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td></td>
</tr>
<tr>
<td>• show monitor all - Displays the mirroring information present in the system.</td>
<td></td>
</tr>
</tbody>
</table>
### 4.108 default exec-timeout

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command configures the default exec-timeout value for line disconnection. This value ranges between 1 and 18000 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>default exec-timeout &lt;integer (1-18000)&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>no default exec-timeout</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product(config)# default exec-timeout 5</code></td>
</tr>
</tbody>
</table>
4.109  **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 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>` - 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

<table>
<thead>
<tr>
<th>Mode</th>
<th>Interface Configuration Mode (VLAN)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The interface should be shutdown before executing this command.</td>
</tr>
</tbody>
</table>

| 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

<table>
<thead>
<tr>
<th>Related Command(s)</th>
<th>* ip address – Configures IP address for an interface.</th>
</tr>
</thead>
</table>

206
### 4.110 clear http server statistics

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command clears the HTTP server requests received and discarded statistics.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>clear http server statistics</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product(config)# clear http server statistics</code></td>
</tr>
</tbody>
</table>
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-transmitting 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.
### CHAPTER : RADIUS

**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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`debug radius {all</td>
</tr>
<tr>
<td>Parameter</td>
<td><strong>Parameter Description</strong></td>
</tr>
<tr>
<td>Description</td>
<td>• <em>all</em> - Generates traces for all the RADIUS server messages</td>
</tr>
<tr>
<td></td>
<td>• <em>errors</em> - 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.</td>
</tr>
<tr>
<td></td>
<td>• <em>events</em> - Generates traces for events related messages. Events like authentication query from authenticator, response from server are registered in the log.</td>
</tr>
<tr>
<td></td>
<td>• <em>packets</em> - Generates traces for number of packets, kind of packets received and sent from server.</td>
</tr>
<tr>
<td></td>
<td>• <em>responses</em> - Generates traces for responses sent from the server to authenticator.</td>
</tr>
<tr>
<td></td>
<td>• <em>timers</em> - Generates traces for the different timers used in the session before the system is reboot.</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Default</td>
<td>Debugging is Disabled</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# debug radius all</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Parameter Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ucast_addr&gt;</code></td>
<td>Displays the related information of the specified unicast address of the RADIUS server host.</td>
</tr>
<tr>
<td><code>&lt;ip6_addr&gt;</code></td>
<td>Displays the related information of the specified IPv6 address of the RADIUS server host.</td>
</tr>
<tr>
<td><code>&lt;string&gt;</code></td>
<td>Displays the name of the RADIUS server host. This maximum value of the string is of size 32.</td>
</tr>
</tbody>
</table>

**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
Chapter 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`
• `debug tacacs`
• `show tacacs`
### 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 <secret key>}
```
```
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` - 40
- `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 debug tacacs

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
</table>
| Syntax            | `debug tacacs { all | info | errors | dumptx | dumprx }`  
`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 unreachable, 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. |
| Mode               | Privileged EXEC Mode |
| Default            | Debugging is Disabled |
| Example            | `Your Product# debug tacacs all` |
6.5 show tacacs

**Command Objective**  This command 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.

**Syntax**  
```bash
show tacacs
```

**Mode**  
Privileged EXEC Mode

It displays the information only for the servers configured in the TACACS server table.

**Example**  
```
Your Product# show tacacs
Server : 1
Server address : 12.0.0.100
Address Type : IPV4
  Single Connection : no
  TCP port : 49
  Timeout : 5
  Secret Key : Supermicro
Server : 2
Server address : 2005::33
Address Type : IPV6
  Single Connection : no
  TCP port : 4949
  Timeout : 5
  Secret Key : Supermicro
Authen. Starts sent : 0
Authen. Continues sent : 0
Authen. Enables sent : 0
Authen. Aborts sent : 0
Authen. Pass rcvd. : 0
Authen. Fails rcvd. : 0
Authen. Get User rcvd. : 0
Authen. Get Pass rcvd. : 0
Authen. Get Data rcvd. : 0
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authen. Errors rcvd.</td>
<td>0</td>
</tr>
<tr>
<td>Authen. Follows rcvd.</td>
<td>0</td>
</tr>
<tr>
<td>Authen. Restart rcvd.</td>
<td>0</td>
</tr>
<tr>
<td>Authen. Sess. timeouts</td>
<td>0</td>
</tr>
<tr>
<td>Author. Requests sent</td>
<td>0</td>
</tr>
<tr>
<td>Author. Pass Add rcvd.</td>
<td>0</td>
</tr>
<tr>
<td>Author. Pass Repl rcvd.</td>
<td>0</td>
</tr>
<tr>
<td>Author. Fails rcvd.</td>
<td>0</td>
</tr>
<tr>
<td>Author. Errors rcvd.</td>
<td>0</td>
</tr>
<tr>
<td>Author Follows rcvd.</td>
<td>0</td>
</tr>
<tr>
<td>Author. Sess. timeouts</td>
<td>0</td>
</tr>
<tr>
<td>Acct. start reqs. sent</td>
<td>0</td>
</tr>
<tr>
<td>Acct. WD reqs. sent</td>
<td>0</td>
</tr>
<tr>
<td>Acct. Stop reqs. sent</td>
<td>0</td>
</tr>
<tr>
<td>Acct. Success rcvd.</td>
<td>0</td>
</tr>
<tr>
<td>Acct. Errors rcvd.</td>
<td>0</td>
</tr>
<tr>
<td>Acct. Follows rcvd.</td>
<td>0</td>
</tr>
<tr>
<td>Acct. Sess. timeouts</td>
<td>0</td>
</tr>
<tr>
<td>Malformed Pkts. rcvd.</td>
<td>0</td>
</tr>
<tr>
<td>Socket failures</td>
<td>0</td>
</tr>
<tr>
<td>Connection failures</td>
<td>0</td>
</tr>
</tbody>
</table>

**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.
Chapter 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`ip ssh {version compatibility</td>
<td>cipher ([des-cbc] [3des-cbc] [aes128-cbc] [aes256-cbc])</td>
</tr>
<tr>
<td>`no ip ssh {version compatibility</td>
<td>cipher ([des-cbc] [3des-cbc] [aes128-cbc] [aes256-cbc])</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td>`ssh {enable</td>
</tr>
</tbody>
</table>
| **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

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your Product# debug ssh all</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>ip ssh transport-max-allowed bytes &lt;integer(1-32768)&gt;</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global configuration Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product# ip ssh transport-max-allowed bytes 1</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>* show ip ssh - Displays SSH server information</td>
</tr>
</tbody>
</table>
## 7.6 ip ssh pubkey-chain

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><strong>ip ssh pubkey-chain</strong></td>
</tr>
<tr>
<td></td>
<td><strong>no ip ssh pubkey-chain</strong></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# ip ssh pubkey-chain</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>* show ip ssh - Displays SSH server information</td>
</tr>
</tbody>
</table>
### 7.7 ssh server-address

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command configures the SSH server listening IP address and the primary port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>ssh server-address &lt;ip-address&gt; [port &lt;integer(1-65535)&gt;]</code></td>
</tr>
<tr>
<td>Parameter Description</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td>Port - 22</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config)# ssh server-address 12.0.0.0 port 1</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td></td>
</tr>
</tbody>
</table>
### 7.8 show ssh-configurations

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays the SSH server listening IP address and port information.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show ssh-configurations</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product# show ssh-configurations</code></td>
</tr>
<tr>
<td></td>
<td>SSH Listening IP 12.0.0.0</td>
</tr>
<tr>
<td></td>
<td>Port 1</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>• <code>ssh server-address</code> - Configures the SSH server listening IP address and the primary port number</td>
</tr>
</tbody>
</table>
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
### 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. |


| 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)]** - Configures the usage key (512 or 1024).

**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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>ssl gen cert-req algo rsa sn &lt;SubjectName&gt;</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product# ssl gen cert-req algo rsa sn 10.6.4.248</code></td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>- <code>show ssl server-cert</code> - Displays SSL server certificate.</td>
</tr>
<tr>
<td></td>
<td>- <code>show ip http secure server status</code> - Displays SSL status and configuration information</td>
</tr>
</tbody>
</table>
### 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

**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

- SSLServer 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@Supermicro.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:
    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:
  Exponent:65537(0x10001)
Signature Algorithm: md5WithRSAEncryption
```
Supermicro Switch Configuration CLI Guide

31:00:bc:9f:00:62:34:d1:15:c0:a4:7e:d9:27:c3:d2:d7:01:
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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays SSL status and configuration information. Information such as HTTP secure server status, http secure server ciphersuite are displayed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>show ip http secure server status</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Note</td>
<td>This command will display output only if http secure server ciphersuite and crypto keys are configured.</td>
</tr>
</tbody>
</table>

#### Example

```
Your Product# show ip http secure server status
HTTP secure server status : Enabled
HTTP secure server ciphersuite : RSA-DES-SHA:RSA-3DES-SHA:RSAEXP1024DES-SHA:
```

#### 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}`

<table>
<thead>
<tr>
<th>Parameter Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Allows configuration to both SSL3 and TLS1 SSL protocols. Server accepts all the connection and the https session is established.</td>
</tr>
<tr>
<td>ssl3</td>
<td>Configures SSL version 3 protocol.</td>
</tr>
<tr>
<td>tls1</td>
<td>Configures Transport Layer Security version 1 protocol.</td>
</tr>
</tbody>
</table>

**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
Chapter 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 snmp broadcast-poll-timeout`
- `set snmp broadcast-delay-time`
- `set snmp multicast-mode send-request`
- `set snmp multicast-poll-timeout`
- `set snmp multicast-delay-time`
- `set snmp multicast-group-address`
- `set snmp manycast-poll-interval`
- `set snmp manycast-poll-timeout`
- `set snmp manycast-poll-retry-count`
- `set snmp manycast-server`
- `show snmp clock`
- `show snmp status`
- `show snmp unicast-mode status`
- `show snmp broadcast-mode status`
- `show snmp multicast-mode status`
- `show snmp manycast-mode status`
- `debug snmp`
- `show snmp statistics`
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 SNTP 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 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.
9.2 set sntp client

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command either enables or disables SNTP client module.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>set sntp client {enabled</td>
</tr>
<tr>
<td>Parameter</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>• enabled</td>
<td>Enables SNTP client module and sends a request to the host for time synchronization.</td>
</tr>
<tr>
<td>• disabled</td>
<td>Disables SNTP client module and no request is sent to the host for time synchronization.</td>
</tr>
<tr>
<td>Mode</td>
<td>SNTP Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config-sntp)# set sntp client enabled</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>• sntp - Enters to SNTP configuration mode</td>
</tr>
<tr>
<td></td>
<td>• show sntp status - Displays the status of SNTP client.</td>
</tr>
</tbody>
</table>
9.3 set sntp client version

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command sets the operating version of the SNTP for the client.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>set sntp client version { v1</td>
</tr>
<tr>
<td>Parameter Description</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• v1 - Sets the version of SNTP client as 1</td>
</tr>
<tr>
<td></td>
<td>• v2 - Sets the version of SNTP client as 2</td>
</tr>
<tr>
<td></td>
<td>• v3 - Sets the version of SNTP client as 3</td>
</tr>
<tr>
<td></td>
<td>• v4 - Sets the version of SNTP client as 4</td>
</tr>
<tr>
<td>Mode</td>
<td>SNTP Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td>v4</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config-sntp)# set sntp client version v3</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>• snmp - Enters to SNTP configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• show snmp status - Displays the status of SNTP client.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command sets the system clock as either AM PM format or HOURS format.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>set sntp client clock-format {ampm</td>
</tr>
<tr>
<td>Parameter Description</td>
<td>• ampm - Sets the system clock in am/ pm format</td>
</tr>
<tr>
<td></td>
<td>• hours - Sets the system clock in 24 hours format</td>
</tr>
<tr>
<td>Mode</td>
<td>SNTP Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td>hours</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config-sntp)# set sntp client clock-format ampm</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>• sntp - Enters to SNTP configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• show sntp status - Displays SNTP status.</td>
</tr>
<tr>
<td></td>
<td>• show sntp clock - Displays the current time.</td>
</tr>
</tbody>
</table>
### 9.7 set sntp client time zone

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command sets the system time zone with respect to UTC. The no form of command resets the system time zone to GMT.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>set sntp client time-zone &lt;UTC-offset value as (+HH:MM /- HH:MM) (+00:00 to +14:00)/ (-00:00 to -12:00)&gt;</code> Eg: +05:30 <code>no sntp client time-zone</code></td>
</tr>
</tbody>
</table>
| 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 servers require 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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>set sntp unicast-poll-interval &lt;value (16-16284) seconds&gt;</code></td>
</tr>
<tr>
<td>Mode</td>
<td>SNTP Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td>64</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config-sntp)# set sntp unicast-poll-interval 50</td>
</tr>
</tbody>
</table>
| 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**

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>set sntp unicast-max-poll-timeout &lt;value (1-30) seconds&gt;</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>SNTP Configuration Mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>5</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product (config-sntp)# set sntp unicast-max-poll-timeout 25</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>* <code>sntp</code> – Enters to SNTP configuration mode.</td>
</tr>
<tr>
<td></td>
<td>* <code>show sntp unicast-mode status</code> - Displays the SNTP Unicast Mode status.</td>
</tr>
</tbody>
</table>
### 9.13 set sntp unicast-max-poll-retry

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>set sntp unicast-max-poll-retry &lt;value (1-10) times&gt;</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>SNTP Configuration Mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><em>Your Product (config-sntp)# set sntp unicast-max-poll-retry 10</em></td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td><em>sntp</em> – Enters to SNTP configuration mode</td>
</tr>
<tr>
<td></td>
<td><em>show sntp unicast-mode status</em> - Displays the SNTP Unicast Mode status.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command either enables or disables the sntp to send status request.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`set sntp broadcast-mode send-request {enabled</td>
</tr>
</tbody>
</table>
| 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**

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>set sntp broadcast-poll-timeout [&lt;value (1-30) seconds&gt;]</code></td>
</tr>
<tr>
<td>Mode</td>
<td>SNTP Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td>5</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config-sntp)# set sntp broadcast-poll-timeout 30</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td></td>
</tr>
</tbody>
</table>
  * sntp – Enters to SNTP configuration mode  
  * show sntp broadcast-mode status – Displays the SNTP broadcast mode status |
## 9.17 set sntp broadcast-delay-time

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td>set sntp broadcast-delay-time [&lt;value (1000-15000) microseconds&gt;]</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>SNTP Configuration Mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>8000</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product (config-sntp)# set sntp broadcast-delay-time 2000</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>* sntp – Enters to SNTP configuration mode</td>
</tr>
<tr>
<td></td>
<td>* show sntp broadcast-mode status – Displays the SNTP broadcast mode status</td>
</tr>
</tbody>
</table>
### 9.18 set sntp multicast-mode send-request

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command sets the status of sending the request to the multicast server to calculate the delay time.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td>`set sntp multicast-mode send-request {enabled</td>
</tr>
</tbody>
</table>
| **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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td>set sntp multicast-poll-timeout [&lt;value (1-30) seconds&gt;]</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>SNTP Configuration Mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>5</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product (config-sntp)# set sntp multicast-poll-timeout 10</td>
</tr>
</tbody>
</table>
| **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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>set sntp multicast-delay-time [&lt;value (1000-15000) microseconds&gt;]</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>SNTP Configuration Mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>8000</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product (config-sntp)# set sntp multicast-delay-time 2000</td>
</tr>
</tbody>
</table>
| **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)**
- **snmp** - 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**

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>set sntp manycast-poll-timeout [&lt;value (1-30) seconds&gt;]</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>SNTP Configuration Mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>5</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product (config-sntp)# set sntp manycast-poll-timeout 10</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td></td>
</tr>
</tbody>
</table>
  - `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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>set sntp manycast-poll-retry-count [&lt;value (1-10)&gt;]</code></td>
</tr>
<tr>
<td>Mode</td>
<td>SNTP Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td>3</td>
</tr>
<tr>
<td>Example</td>
<td><code>Your Product (config-sntp)# set sntp manycast-poll-retry-count 5</code></td>
</tr>
<tr>
<td>Related Command(s)</td>
<td></td>
</tr>
</tbody>
</table>
  * `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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command configures SNTP multicast or broadcast server address in manycast mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>set sntp manycast-server { broadcast</td>
</tr>
</tbody>
</table>
| Parameter Description | • broadcast - Configures SNTP broadcast server address in manycast mode  
|                    | • multicast - Configures SNTP multicast server address in manycast mode.  
|                    | • ipv4 \(<\text{mcast\_addr}>\) - Sets the multicast server address in internet  
|                    |   protocol v4.  
|                    | • ipv6 \(<\text{ip6\_addr}>\) - Sets the multicast server address in internet  
|                    |   protocol v6.  |
| Mode              | SNTP Configuration Mode |
| Example           | Your Product (config-sntp)# set sntp manycast-server \multi\_cast 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**

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays the current time.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show sntp clock</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>User / Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product# show sntp clock</td>
</tr>
<tr>
<td></td>
<td>current time : Sat Jan  01 2000 00:07:04 (UTC + 0:0)</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>set sntp client clock-format - Sets the system clock as either AM PM format or HOURS format.</td>
</tr>
</tbody>
</table>
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-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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the status of SNTP in broadcast mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show sntp broadcast-mode status</code></td>
</tr>
<tr>
<td>Mode</td>
<td>User / Privileged EXEC Mode</td>
</tr>
<tr>
<td></td>
<td>This command is executed only if the addressing mode is set as broadcast.</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# show sntp broadcast-mode status</td>
</tr>
<tr>
<td></td>
<td>send sntp request to server in broadcast mode is disabled</td>
</tr>
<tr>
<td></td>
<td>broadcast poll time out value is 5</td>
</tr>
<tr>
<td></td>
<td>broadcast delay time value is 8000</td>
</tr>
<tr>
<td></td>
<td>broadcast sntp server is 12.0.0.100</td>
</tr>
</tbody>
</table>

**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.
CHAPTER: SNTP

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
```

---

281
# 9.33 show sntp statistics

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the sntp packet statistics.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>show sntp statistics</td>
</tr>
<tr>
<td>Mode</td>
<td>User / Privilege EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# show sntp statistics</td>
</tr>
<tr>
<td></td>
<td>Number of SNTP server-reply Received : 0</td>
</tr>
<tr>
<td></td>
<td>Number of SNTP client-request Transmitted : 0</td>
</tr>
<tr>
<td></td>
<td>Number of SNTP Pkt InDiscards : 0</td>
</tr>
</tbody>
</table>
Chapter 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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command disables agentx-subagent.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>disable snmpsubagent</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product (config)# disable snmpsubagent</code></td>
</tr>
</tbody>
</table>

**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`

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>enable snmpagent</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>SNMP agent is enabled.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product (config)# enable snmpagent</code></td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>- <code>enable snmpsubagent</code> - Enables agentx-subagent capabilities.</td>
</tr>
<tr>
<td></td>
<td>- <code>disable snmpagent</code> - Disables SNMP agent.</td>
</tr>
</tbody>
</table>
### 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`

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command configures the SNMP community details. The no form of this command removes the SNMP community details.</th>
</tr>
</thead>
</table>
| 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**

<table>
<thead>
<tr>
<th>Command Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command configures SNMP group details. The no form of the command removes the SNMP group details.</td>
</tr>
</tbody>
</table>

**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 an 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
```
CHAPTER : SNMPV3

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}]
```
```
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 version.
  - `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` keyword.
- `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.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Global Configuration Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>Group Name</td>
<td>iso</td>
</tr>
<tr>
<td>Read/Write/Notify view</td>
<td>iso</td>
</tr>
<tr>
<td>Storage Type</td>
<td>volatile</td>
</tr>
<tr>
<td>Row status</td>
<td>Active</td>
</tr>
<tr>
<td>Group Name</td>
<td>initial</td>
</tr>
<tr>
<td>Read/Write/Notify View</td>
<td>restricted</td>
</tr>
<tr>
<td>Storage Type</td>
<td>non-volatile</td>
</tr>
<tr>
<td>Group Name</td>
<td>Initial</td>
</tr>
<tr>
<td>Read/Write/Notify View</td>
<td>iso</td>
</tr>
<tr>
<td>Storage Type</td>
<td>non-volatile</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command configures the proxy.</td>
</tr>
</tbody>
</table>

The no form of the command removes the proxy.

**Syntax**

```clish
no snmp proxy name <ProxyName>
```

<table>
<thead>
<tr>
<th>Parameter Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>&lt;ProxyName&gt;</strong> - Identifies an entry in the proxy table.</td>
</tr>
<tr>
<td>This will be the INDEX used for the Proxy Table.</td>
</tr>
<tr>
<td><strong>ProxyType</strong> - Forwards the messages using the translation parameters defined by proxy entry. The list contains. Options are:</td>
</tr>
<tr>
<td>- <strong>Read</strong> - Forwards the read messages to get the request from the manager.</td>
</tr>
<tr>
<td>- <strong>Write</strong> - Forwards the write messages to set configurations.</td>
</tr>
<tr>
<td>- <strong>Inform</strong> - Forwards the notification messages to the agent.</td>
</tr>
<tr>
<td>- <strong>Trap</strong> - Forwards the SNMP trap messages to the agent</td>
</tr>
<tr>
<td><strong>ContextEngineID &lt;EngineId&gt;</strong> - Configures an context engine ID of the agent with whom the manager communicates through the proxy.</td>
</tr>
<tr>
<td><strong>TargetParamsIn &lt;TargetParam&gt;</strong> - Configures the SNMP version that the manager sends as request to the proxy.</td>
</tr>
<tr>
<td><strong>TargetOut &lt;TargetOut&gt;</strong> - Configures the SNMP version that the proxy uses to communicate with multiple agent .</td>
</tr>
<tr>
<td>This object is only used when selection of a single target is required (that is, when forwarding an incoming read or write request).</td>
</tr>
<tr>
<td><strong>ContextName &lt;ProxyContextName&gt;</strong> - Configures an 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.</td>
</tr>
<tr>
<td><strong>Storage Type</strong> - Sets the required storage type for the group entry</td>
</tr>
<tr>
<td>- <strong>volatile</strong> - Sets the storage type as temporary. Erases the configuration setting on restarting the system.</td>
</tr>
<tr>
<td>- <strong>nonvolatile</strong> - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.</td>
</tr>
</tbody>
</table>
### 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`

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command configures the mib proxy. The no form of the command removes the mib proxy.</th>
</tr>
</thead>
</table>
| Syntax | `snmp mibproxy name <ProxyName> ProxyType {Read | Write | inform | Trap} mibid <MibId> TargetParamsIn <TargetParam> TargetOut <TargetOut> [StorageType {volatile | nonvolatile}]`
| no form | `no snmp mibproxy name <ProxyName>` |

<table>
<thead>
<tr>
<th>Parameter Description</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ProxyName&gt;</code></td>
<td>- Identifies an entry in the proxy table. This will be the INDEX used for the Proxy Table.</td>
<td></td>
</tr>
<tr>
<td><code>ProxyType</code></td>
<td>- Forwards the messages using the translation parameters defined by proxy entry. The list contains:. Options are:</td>
<td></td>
</tr>
<tr>
<td><code>Read</code></td>
<td>- Forwards the read messages to get the request from the manager.</td>
<td></td>
</tr>
<tr>
<td><code>Write</code></td>
<td>- Forwards the write messages to set configurations.</td>
<td></td>
</tr>
<tr>
<td><code>Inform</code></td>
<td>- Forwards the notification messages to the agent.</td>
<td></td>
</tr>
<tr>
<td><code>Trap</code></td>
<td>- Forwards the SNMP trap messages to the agent.</td>
<td></td>
</tr>
<tr>
<td><code>Mibid &lt;MibId&gt;</code></td>
<td>- Configures an context MIB ID of the agent with whom the manager communicates through the proxy.</td>
<td></td>
</tr>
<tr>
<td><code>TargetParamsIn&lt;TargetParam&gt;</code></td>
<td>- Configures the SNMP version that the manager sends as request to the proxy.</td>
<td></td>
</tr>
<tr>
<td><code>TargetOut&lt;TargetOut&gt;</code></td>
<td>- 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).</td>
<td></td>
</tr>
<tr>
<td><code>Storage Type</code></td>
<td>- Storage type. Options are:</td>
<td></td>
</tr>
<tr>
<td><code>volatile</code></td>
<td>- Sets the storage type as temporary. Erases the configuration setting on restarting the system.</td>
<td></td>
</tr>
<tr>
<td><code>nonvolatile</code></td>
<td>- Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.</td>
<td></td>
</tr>
</tbody>
</table>

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
**CHAPTER : SNMPV3**

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 a IP target address to which the generated SNMP notifications are sent.
- `IP6Address` - Configures a 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
CHAPTER : SNMPV3

10.13 \textbf{snmp targetparams}

\begin{tabular}{|p{5cm}|p{15cm}|}
\hline
\textbf{Command Objective} & This command configures the SNMP target parameters. The no form of the command removes the SNMP target parameters. \\
\hline
\textbf{Syntax} & \texttt{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\}]
\texttt{no snmp targetparams <ParamName>}
\hline
\textbf{Parameter Description} & \begin{itemize}
\item \texttt{<ParamName>} - Sets a unique identifier of the parameter.
\item \texttt{User <UserName>} - Sets an user for which the target parameter is to be done.
\item \texttt{security-model} - Sets the security model
\item \texttt{v1} – Sets the SNMP version as Version 1.
\item \texttt{v2c} – Sets the SNMP version as Version 2.
\item \texttt{v3} – Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word
\item \texttt{auth} - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication
\item \texttt{noauth} - Sets no-authentication
\item \texttt{priv} - Specifies both authentication and privacy
\item \texttt{message-processing} - Sets the message processing model
\hspace{1cm} – \texttt{v1} – Sets the SNMP version as Version 1.
\hspace{1cm} – \texttt{v2c} – Sets the SNMP version as Version 2.
\hspace{1cm} – \texttt{v3} – Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word
\item \texttt{volatile} - Sets the storage type as temporary. Erases the configuration setting on restarting the system
\item \texttt{nonvolatile} - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration can be viewed on restarting the system.
\end{itemize}
\hline
\end{tabular}
• `filterprofile-name <profilenname>` - 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 SNMP 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
### SNMPV3

#### 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 an 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
```
no snmp filterprofile <profile-name> <OIDTree> [mask <OIDMask>] {included | excluded} [{volatile | nonvolatile}]
```
```
no snmp filterprofile <profile-name> <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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command enables generation of authentication traps from the snmp agent (for all snmpv1, snmpv2 and snmpv3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><strong>snmp-server enable traps snmp authentication</strong></td>
</tr>
<tr>
<td></td>
<td><strong>no snmp-server enable traps snmp authentication</strong></td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config)# snmp-server enable traps snmp authentication</td>
</tr>
</tbody>
</table>
### 10.18  `snmp-server trap udp-port`

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
</table>
| 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. |

---

*Supermicro Switch Configuration CLI Guide*
### 10.19 `snmp-server trap proxy-udp-port`

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
</table>
| **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**

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command configures the agent port on which agent listens. The port number value ranges between 1 and 65535.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>snmp agent port &lt;port&gt;</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>161</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product (config)# snmp agent port 100</code></td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>* <code>show snmp</code> - Displays the status information of SNMP communications</td>
</tr>
</tbody>
</table>
### 10.21 `snmp tcp enable`

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command enables sending snmp messages over tcp. The no form of the command disables sending snmp messages over tcp.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>snmp tcp enable</code></td>
</tr>
<tr>
<td></td>
<td><code>no snmp tcp enable</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product (config)# snmp tcp enable</code></td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>- <code>show snmp tcp</code> - Displays the configuration for snmp over tcp.</td>
</tr>
</tbody>
</table>
### 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`

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>snmp-server tcp-port &lt;port&gt;</code></td>
</tr>
<tr>
<td>no <code>snmp-server tcp-port</code></td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td>161</td>
</tr>
<tr>
<td>Example</td>
<td><code>Your Product (config)# snmp-server tcp-port 161</code></td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>• <code>show snmp tcp</code> - Displays the configuration for snmp over tcp.</td>
</tr>
<tr>
<td><strong>10.24</strong></td>
<td><strong>snmp-server trap tcp-port</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Command Objective</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
| **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. |
This command enables generation of a particular trap. The no form of the command disables generation of a particular trap.

**Syntax**

```plaintext
snmp-server enable traps { [firewall-limit] [linkup] [linkdown] [sip-states] [sip-cfg-change] [coldstart] [poe-power] [dhcp-pool-limit] [dsxl-line] }
```

```plaintext
no snmp-server enable traps { [firewall-limit] [linkup] [linkdown] [sip-states] [sip-cfg-change] [coldstart] [poe-power] [dhcp-pool-limit] [dsxl-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
- **dsxl-line** - Generates a trap for all the DSX1 line trap

**Mode**

Global Configuration Mode

**Example**

```plaintext
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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays global information of SNMP Agentx communications.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>show snmp agentx information</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# show snmp agentx information</td>
</tr>
<tr>
<td></td>
<td>Agentx Subagent is enabled</td>
</tr>
<tr>
<td></td>
<td>TransportDomain :TCP</td>
</tr>
<tr>
<td></td>
<td>Master IP Address :10.0.0.2</td>
</tr>
<tr>
<td></td>
<td>Master PortNo :705</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>• enable snmpsubagent - Enables agentx-subagent capabilities.</td>
</tr>
<tr>
<td></td>
<td>• disable snmpsubagent - Disables agentx-subagent.</td>
</tr>
<tr>
<td></td>
<td>• disable snmpagent - Disables SNMP agent.</td>
</tr>
</tbody>
</table>
10.27 show snmp agentx statistics

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays all the information regarding SNMP Agentx statistics.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show snmp agentx statistics</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product# show snmp agentx statistics</td>
</tr>
</tbody>
</table>

```
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
UnRegister PDU      : 0
Close PDU           : 0
Response PDU        : 837

Rx Statistics
Rx Packets          : 859
Get PDU             : 1
GetNext PDU         : 836
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           : 0
Response PDU        : 21
```
**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**

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the configured SNMP community details.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show snmp community</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# show snmp community</td>
</tr>
<tr>
<td></td>
<td>Community Index: NETMAN</td>
</tr>
<tr>
<td></td>
<td>Community Name: NETMAN</td>
</tr>
<tr>
<td></td>
<td>Security Name: none</td>
</tr>
<tr>
<td></td>
<td>Context Name:</td>
</tr>
<tr>
<td></td>
<td>Transport Tag:</td>
</tr>
<tr>
<td></td>
<td>Storage Type: volatile</td>
</tr>
<tr>
<td></td>
<td>Row Status: active</td>
</tr>
<tr>
<td></td>
<td>==============================================================</td>
</tr>
<tr>
<td></td>
<td>Community Index: PUBLIC</td>
</tr>
<tr>
<td></td>
<td>Community Name: PUBLIC</td>
</tr>
<tr>
<td></td>
<td>Security Name: none</td>
</tr>
<tr>
<td></td>
<td>Context Name:</td>
</tr>
<tr>
<td></td>
<td>Transport Tag:</td>
</tr>
<tr>
<td></td>
<td>Storage Type: volatile</td>
</tr>
<tr>
<td></td>
<td>Row Status: active</td>
</tr>
</tbody>
</table>

**Related Command(s)**

- `snmp community index` - Configures the SNMP community details
10.30  **show snmp group**

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the configured SNMP groups.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show snmp group</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the configured SNMP group access details.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show snmp group access</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# show snmp group access</td>
</tr>
</tbody>
</table>

```
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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays the Engine Identifier.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show snmp engineID</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product# <code>show snmp engineID</code></td>
</tr>
<tr>
<td></td>
<td><code>EngineId: 80.00.08.1c.04.46.53</code></td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>snmp engineid</code> - Configures the engine identifier</td>
</tr>
<tr>
<td></td>
<td>• <code>snmp user</code> - Configures the SNMP user details</td>
</tr>
</tbody>
</table>
## 10.33 show snmp proxy

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays proxy details.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show snmp proxy</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
</tbody>
</table>

### 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**

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays the configured SNMP Tree views.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show snmp viewtree</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product# show snmp viewtree</td>
</tr>
<tr>
<td></td>
<td>View Name: iso</td>
</tr>
<tr>
<td></td>
<td>Subtree OID: 1</td>
</tr>
<tr>
<td></td>
<td>Subtree Mask:</td>
</tr>
<tr>
<td></td>
<td>View Type: included</td>
</tr>
<tr>
<td></td>
<td>Storage Type: nonVolatile</td>
</tr>
<tr>
<td></td>
<td>Row Status: active</td>
</tr>
<tr>
<td></td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>View Name: restricted</td>
</tr>
<tr>
<td></td>
<td>Subtree OID: 1</td>
</tr>
<tr>
<td></td>
<td>Subtree Mask:</td>
</tr>
<tr>
<td></td>
<td>View Type: included</td>
</tr>
<tr>
<td></td>
<td>Storage Type: nonVolatile</td>
</tr>
<tr>
<td></td>
<td>Row Status: active</td>
</tr>
<tr>
<td></td>
<td>------------------------------------------------------</td>
</tr>
</tbody>
</table>

**Related Command(s)**

- `snmp access` - Configures the SNMP group access details
- `snmp view` - Configures the SNMP view
### 10.36 show snmp targetaddr

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the configured SNMP target Addresses.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td>show snmp targetaddr</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product# show snmp targetaddr</td>
</tr>
<tr>
<td></td>
<td>Target Address Name : ht231</td>
</tr>
<tr>
<td></td>
<td>IP Address : 12.0.0.100</td>
</tr>
<tr>
<td></td>
<td>Port : 150</td>
</tr>
<tr>
<td></td>
<td>Tag List : tg231</td>
</tr>
<tr>
<td></td>
<td>Parameters : pa231</td>
</tr>
<tr>
<td></td>
<td>Storage Type : Non-volatile</td>
</tr>
<tr>
<td></td>
<td>Row Status : Active</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the configured SNMP Target Address Params.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>show snmp targetparam</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# show snmp targetparam</td>
</tr>
</tbody>
</table>

```plaintext
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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the configured SNMP users.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><strong>show snmp user</strong></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# show snmp user</td>
</tr>
<tr>
<td></td>
<td>Engine ID: 80.00.08.1c.04.46.53</td>
</tr>
<tr>
<td></td>
<td>User: initial</td>
</tr>
<tr>
<td></td>
<td>Authentication Protocol: none</td>
</tr>
<tr>
<td></td>
<td>Privacy Protocol: none</td>
</tr>
<tr>
<td></td>
<td>Storage Type: nonVolatile</td>
</tr>
<tr>
<td></td>
<td>Row Status: active</td>
</tr>
<tr>
<td></td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Engine ID: 80.00.08.1c.04.46.53</td>
</tr>
<tr>
<td></td>
<td>User: templateMD5</td>
</tr>
<tr>
<td></td>
<td>Authentication Protocol: MD5</td>
</tr>
<tr>
<td></td>
<td>Privacy Protocol: none</td>
</tr>
<tr>
<td></td>
<td>Storage Type: nonVolatile</td>
</tr>
<tr>
<td></td>
<td>Row Status: active</td>
</tr>
<tr>
<td></td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Engine ID: 80.00.08.1c.04.46.53</td>
</tr>
<tr>
<td></td>
<td>User: templateSHA</td>
</tr>
<tr>
<td></td>
<td>Authentication Protocol: SHA</td>
</tr>
<tr>
<td></td>
<td>Privacy Protocol: DES_CBC</td>
</tr>
<tr>
<td></td>
<td>Storage Type: nonVolatile</td>
</tr>
<tr>
<td></td>
<td>Row Status: active</td>
</tr>
<tr>
<td></td>
<td>------------------------------------------------</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays the configured SNMP Notification types.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show snmp notif</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the inform message statistics.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show snmp inform statistics</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the proxy udp port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>show snmp-server proxy-udp-port</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
</tbody>
</table>
| 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.
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] |
|------------|--------------------------------------|

- **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`

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command gets the next mib object for the given object.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command is intended for internal testing purpose only</td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
<td>`snmpgetnext mib {name</td>
</tr>
<tr>
<td><strong>Parameter Description</strong></td>
<td></td>
</tr>
<tr>
<td>• name &lt;value&gt; - Gets the next mib object name. This is a string value with maximum size as 32.</td>
<td></td>
</tr>
<tr>
<td>• oid &lt;value&gt; - Gets the next mib object identifier. This is a string value with maximum size as 32.</td>
<td></td>
</tr>
<tr>
<td>• short - Displays the value of the mib object.</td>
<td></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product (config)# snmpgetnext mib name fspbgp4PeerExtTable short</code></td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td></td>
</tr>
<tr>
<td>• <code>show snmp</code> - Displays the status information of SNMP communications.</td>
<td></td>
</tr>
</tbody>
</table>
### 10.48 snmpwalk mib

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays all the mib objects of the given table.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command is intended for internal testing purpose only</td>
</tr>
<tr>
<td>Syntax</td>
<td>`snmpwalk mib {name</td>
</tr>
<tr>
<td></td>
<td>[short]</td>
</tr>
<tr>
<td>Parameter Description</td>
<td></td>
</tr>
<tr>
<td>name &lt;value&gt;</td>
<td>Gets the next mib object name for the given mib object name. This is a string value with maximum size as 32.</td>
</tr>
<tr>
<td>oid &lt;value&gt;</td>
<td>Gets the next mib object identifier for the given mib object identifier.</td>
</tr>
<tr>
<td>count &lt;integer(1-100)&gt;</td>
<td>Sets the number of entries to be displayed in the mib object. This value ranges between 1 and 100.</td>
</tr>
<tr>
<td>short</td>
<td>Displays the value of the mib object.</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Example</td>
<td><code>Your Product (config)# snmpwalk mib name fsbgp4PeerExtTable</code></td>
</tr>
</tbody>
</table>

---

Example:

```
Your Product (config)# snmpwalk mib name fsbgp4PeerExtTable
```
### 10.49 snmp filter trap

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command sets the traps to be filtered. The no form of the command removes the traps from filter table.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>snmp filter trap {name</td>
</tr>
<tr>
<td></td>
<td>no snmp filter trap {name</td>
</tr>
<tr>
<td>Parameter Description</td>
<td>• name &lt;name&gt;  - Gets the mib object name. This is a string value with maximum size as 32.</td>
</tr>
<tr>
<td></td>
<td>• oid &lt;oid&gt;  - Gets the mib object identifier.</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config)# snmp filter trap name fsbgp4PeerExtTable</td>
</tr>
</tbody>
</table>
# 10.50 show mib oid

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the OID (Object Identifier) of the corresponding mib object name.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command is intended for internal testing purpose only</td>
</tr>
<tr>
<td>Syntax</td>
<td><code>show mib oid &lt;object name. eg ifMainRowStatus&gt;</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td><code>Your Product (config)# show mib oid f sbgp4PeerExtTable</code></td>
</tr>
<tr>
<td></td>
<td>MIB OID for f sbgp4PeerExtTable is 1.3.6.1.4.1.2076.41.2</td>
</tr>
</tbody>
</table>

| Related Command(s) | `snmpset mib` - Sets the value of the mib object via SNMP agent. |
10.51  
**show mib name**

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays the name of the corresponding mib object identifier.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command is intended for internal testing purpose only</td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
<td>show mib name &lt;Object OID. eg 1.3.6.1.6&gt;</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product (config)# show mib name 1.3.6.1.4.1.2076.41.2</td>
</tr>
<tr>
<td></td>
<td>MIB Name for 1.3.6.1.4.1.2076.41.2 is fsbqp4PeerExtTable</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>•  snmpset mib - Sets the value of the mib object via SNMP agent.</td>
</tr>
</tbody>
</table>
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 the industrial 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, local6, local7.

- **severity** - Message severity level. Messages with severity level equal to or higher 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 higher 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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>sender mail-id &lt;mail-id (100)&gt;</code>&lt;br&gt;<code>no sender mail-id</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td><code>syslog@supermicro.com</code></td>
</tr>
<tr>
<td>Note</td>
<td>This command can be executed only if the mail server is configured.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product (config)# sender mail-id <a href="mailto:plabinik@supermicro.com">plabinik@supermicro.com</a></td>
</tr>
</tbody>
</table>

**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
- `receivever 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
```
cmpd <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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command clears the system syslog buffers.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>clear logs</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product (config)# clear logs</code></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td>syslog mail</td>
</tr>
<tr>
<td></td>
<td>no syslog mail</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product (config)# syslog mail</td>
</tr>
</tbody>
</table>
| **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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>syslog localstorage</td>
</tr>
<tr>
<td></td>
<td>no syslog localstorage</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config)# syslog localstorage</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>show syslog local storage - Displays the syslog local storage.</td>
</tr>
<tr>
<td></td>
<td>syslog filename-one - Configures the file name to store the syslog messages.</td>
</tr>
<tr>
<td></td>
<td>syslog filename-two - Configures the file name to store the syslog messages.</td>
</tr>
<tr>
<td></td>
<td>syslog filename-three - Configures the file name to store the syslog messages</td>
</tr>
<tr>
<td></td>
<td>logging-file - Adds an entry in to file table</td>
</tr>
<tr>
<td></td>
<td>show syslog file-name - Displays all the syslog local storage file names.</td>
</tr>
<tr>
<td></td>
<td>show syslog information - Displays the status of consolidated syslog log information.</td>
</tr>
</tbody>
</table>
11.9 syslog filename-one

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command configures a first file to store the syslog messages locally. The maximum size of the file name is 32.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>syslog filename-one &lt;string(32)&gt;</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td></td>
<td>This command is executed only if syslog local storage is enabled.</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config)# syslog filename-one smis1</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>* syslog local storage - Enables the syslog local storage</td>
</tr>
<tr>
<td></td>
<td>* logging-file - Adds an entry in to file table</td>
</tr>
<tr>
<td></td>
<td>* show syslog local storage - Displays the syslog local storage.</td>
</tr>
<tr>
<td></td>
<td>* show logging-file - Displays the Syslog file table</td>
</tr>
<tr>
<td></td>
<td>* show syslog file-name - Displays all the syslog local storage file names.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command configures a third file name to store the syslog messages locally. The maximum size of the file name is 32.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>syslog filename-three &lt;string(32)&gt;</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td></td>
<td>This command is executed only if syslog local storage is enabled.</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config)# syslog filename-three smis3</td>
</tr>
</tbody>
</table>
| 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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>syslog relay-port &lt;integer(0-65535)&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>no syslog relay-port</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>514</td>
</tr>
<tr>
<td></td>
<td>This command is executed only if syslog relay is enabled.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product (config)# syslog relay-port 500</code></td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>* <code>syslog relay</code> - Changes the syslog role from device to relay</td>
</tr>
<tr>
<td></td>
<td>* <code>syslog relay transport type</code> - Sets the syslog relay transport type either as udp or tcp</td>
</tr>
<tr>
<td></td>
<td>* <code>show syslog relay - port</code> - Displays the syslog relay port</td>
</tr>
<tr>
<td></td>
<td>* <code>show syslog relay transport type</code> - Displays the Syslog relay transport type</td>
</tr>
</tbody>
</table>
11.13 syslog profile

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command sets the profile for reliable syslog. The no form of command sets the profile to default (raw) for Reliable Syslog.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`syslog profile {raw</td>
</tr>
<tr>
<td>Parameter Description</td>
<td>* <code>raw</code> - Sets the syslog profile as raw which is the profile for the transport type beep. * <code>cooked</code> - Sets the syslog profile as cooked. This feature is not supported. It may be implemented in the future.</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Default</td>
<td>Raw</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config)# syslog profile raw</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>* <code>show syslog profile</code> - Displays the Syslog profile.</td>
</tr>
</tbody>
</table>
11.14 **logging-file**

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command adds an entry in the file table. The no form of command deletes an entry from the file table.</th>
</tr>
</thead>
</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**

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command configures a server table to log an entry in it. The no form of command deletes an entry from the server table.</th>
</tr>
</thead>
</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**  
```plaintext  
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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command sets the Syslog relay transport type either as udp or tcp.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td>`syslog relay transport type {udp</td>
</tr>
<tr>
<td><strong>Parameter Description</strong></td>
<td>• udp - Sets the relay transport type as udp</td>
</tr>
<tr>
<td></td>
<td>• tcp - Sets the relay transport type as tcp</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product (config)# <code>syslog relay transport type udp</code></td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>• syslog relay – Changes the syslog role from device to relay</td>
</tr>
<tr>
<td></td>
<td>• show syslog role – Displays the syslog role.</td>
</tr>
<tr>
<td></td>
<td>• syslog relay - port – Sets the syslog port through which it receives the syslog messages</td>
</tr>
<tr>
<td></td>
<td>• show syslog relay transport type – Displays the Syslog relay transport type</td>
</tr>
<tr>
<td></td>
<td>• show syslog relay – port – Displays the Syslog relay port.</td>
</tr>
</tbody>
</table>
11.18 show logging

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays all the logging status and configuration information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show logging</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
</tbody>
</table>

```
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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays configurations related to email alerts.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show email alerts</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td></td>
<td>This command is executed only if mail server is configured.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product# show email alerts</code></td>
</tr>
<tr>
<td></td>
<td><code>Sender email-id    : plabinik@Aricent.com</code></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays the syslog role.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show syslog role</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>Your Product# show syslog role</code></td>
</tr>
<tr>
<td></td>
<td><code>Syslog Role : Relay</code></td>
</tr>
</tbody>
</table>

**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*

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays status of the mail option in syslog.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show syslog mail</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><em>Your Product# show syslog mail</em></td>
</tr>
<tr>
<td></td>
<td><em>Syslog Mail Option : Enabled</em></td>
</tr>
</tbody>
</table>

**Related Command(s)**
- `syslog mail` – Enables the mail option in syslog
### 11.22 show syslog localstorage

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the syslog local storage.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show syslog localstorage</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td><code>Your Product# show syslog localstorage</code></td>
</tr>
<tr>
<td></td>
<td><code>Syslog Localstorage : Enabled</code></td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the priority and file name of all the three files configured in the syslog file table.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show logging-file</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product# <code>show logging-file</code>&lt;br&gt;Syslog File Table Information&lt;br&gt;----------------------------&lt;br&gt;PRIORITY   FILE-NAME&lt;br&gt;--------   ----------&lt;br&gt;134         smis1&lt;br&gt;134         smis2&lt;br&gt;134         smis3</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>* <strong>syslog</strong> - Configures the first file to store the syslog messages locally &lt;br&gt;* <strong>syslog filename-two</strong> - Configures the second file name to store the syslog messages locally &lt;br&gt;* <strong>syslog filename-three</strong> - Configures the third file name to store the syslog messages locally &lt;br&gt;* <strong>logging-file</strong> - Adds an entry in to file table</td>
</tr>
</tbody>
</table>
### 11.24 show logging-server

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the information about the syslog logging server table.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>show logging-server</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# show logging-server</td>
</tr>
<tr>
<td></td>
<td>Syslog Forward Table Information</td>
</tr>
<tr>
<td></td>
<td>---------------------------------- --------- ---------- ---- --------</td>
</tr>
<tr>
<td>Priority</td>
<td>Address-Type</td>
</tr>
<tr>
<td>129</td>
<td>ipv4</td>
</tr>
<tr>
<td>134</td>
<td>ipv4</td>
</tr>
</tbody>
</table>

**Related Command(s)**
- logging server - Adds an entry in to logging-server table
11.25 **show mail-server**

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the information about the syslog mail server table.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show mail-server</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
</tbody>
</table>

**Example**

```
Your Product# show mail-server

Syslog Mail Table Information
----------------------------
Priority Address-Type IpAddress Receiver Mail-Id
------------------- ---- --------  -------------------- ----
3 ipv4 23.78.67.89 support1@supermicro.com
13 ipv4 23.78.67.89 support1@supermicro.com
190 ipv4 23.78.67.89 support@supermicro.com
```

**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`

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the syslog profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show syslog profile</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td><code>Your Product# show syslog profile</code></td>
</tr>
<tr>
<td></td>
<td><code>Syslog Profile : raw</code></td>
</tr>
<tr>
<td>Related Command(s)</td>
<td><code>syslog profile</code> - Sets the profile for reliable syslog</td>
</tr>
</tbody>
</table>
# 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
### show syslog file-name

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays all the syslog local storage file names.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show syslog file-name</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# show syslog file-name</td>
</tr>
<tr>
<td></td>
<td>Syslog File Name</td>
</tr>
<tr>
<td></td>
<td>----------------------</td>
</tr>
<tr>
<td></td>
<td>Syslog File-One :smis1</td>
</tr>
<tr>
<td></td>
<td>Syslog File-Two :smis2</td>
</tr>
<tr>
<td></td>
<td>Syslog File-Three :smis3</td>
</tr>
</tbody>
</table>

### 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
CHAPTER: SYSLOG

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**
```plaintext
smtp authentication {auth-login | auth-plain | cram-md5 | digest-md5}
```

```plaintext
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**
```plaintext
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`

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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.</th>
</tr>
</thead>
</table>
| **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` |
Chapter 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-end communication.

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
PassiveOpens : 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
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: 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: 0
Current Estab: 0
Input Segments: 0
<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Segments</td>
<td>0</td>
</tr>
<tr>
<td>Retransmitted Segments</td>
<td>0</td>
</tr>
<tr>
<td>Input Errors</td>
<td>0</td>
</tr>
<tr>
<td>TCP Segments with RST flag Set</td>
<td>0</td>
</tr>
<tr>
<td>HC Input Segments</td>
<td>0</td>
</tr>
<tr>
<td>HC Output Segments</td>
<td>0</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the information such as Local IP Address Type, Local IP and Local Port for each listeners in the network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>show tcp listeners [vrf &lt;vrf-name&gt;]</td>
</tr>
<tr>
<td>Parameter Description</td>
<td>vrf &lt;vrf-name&gt; - 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</td>
</tr>
<tr>
<td></td>
<td>⚖ 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</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# show tcp listeners</td>
</tr>
<tr>
<td></td>
<td>Context Name : default</td>
</tr>
<tr>
<td></td>
<td>TCP Listeners</td>
</tr>
<tr>
<td></td>
<td>================</td>
</tr>
<tr>
<td></td>
<td>Local IP Address Type : 0</td>
</tr>
<tr>
<td></td>
<td>Local IP : 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>Local Port : 22</td>
</tr>
<tr>
<td></td>
<td>Local IP Address Type : 0</td>
</tr>
<tr>
<td></td>
<td>Local IP : 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>Local Port : 23</td>
</tr>
<tr>
<td></td>
<td>Local IP Address Type : 0</td>
</tr>
<tr>
<td></td>
<td>Local IP : 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>Local Port : 80</td>
</tr>
<tr>
<td></td>
<td>Address Type [0 - IPv4 and IPv6] [1 - IPv4] [2 - IPv6]</td>
</tr>
<tr>
<td></td>
<td>Context Name : vrf1</td>
</tr>
<tr>
<td></td>
<td>Context Name : vrf2</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>This command displays the tcp retransmission details.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show tcp retransmission details [vrf &lt;vrf-name&gt;]</code></td>
</tr>
<tr>
<td><strong>Parameter Description</strong></td>
<td><code>vrf &lt;vrf-name&gt;</code> - 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.</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product# show tcp retransmission details</td>
</tr>
<tr>
<td></td>
<td>Context Name : default</td>
</tr>
<tr>
<td></td>
<td>RTO Algorithm Used : VAN JACOBSON</td>
</tr>
<tr>
<td></td>
<td>Min Retransmission Timeout : 0 msec</td>
</tr>
<tr>
<td></td>
<td>Max Retransmission Timeout : 0 msec</td>
</tr>
<tr>
<td></td>
<td>Context Name : vrf1</td>
</tr>
<tr>
<td></td>
<td>RTO Algorithm Used : VAN JACOBSON</td>
</tr>
<tr>
<td></td>
<td>Min Retransmission Timeout : 0 msec</td>
</tr>
<tr>
<td></td>
<td>Max Retransmission Timeout : 0 msec</td>
</tr>
<tr>
<td></td>
<td>Context Name : vrf2</td>
</tr>
<tr>
<td></td>
<td>RTO Algorithm Used : VAN JACOBSON</td>
</tr>
<tr>
<td></td>
<td>Min Retransmission Timeout : 0 msec</td>
</tr>
<tr>
<td></td>
<td>Max Retransmission Timeout : 0 msec</td>
</tr>
<tr>
<td></td>
<td>Context Name : vrf3</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command configures the maximum number of retries for re-transmission in TCP module.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>tcp max retries &lt;integer(1-12)&gt; [vrf &lt;vrf-name&gt;]</code></td>
</tr>
<tr>
<td>Parameter</td>
<td>· <code>&lt;integer(1-12)&gt;</code> - Configures the maximum number of retries done by TCP module. This value ranges between 1 and 12.</td>
</tr>
<tr>
<td>Description</td>
<td>· <code>&lt;vrf &lt;vrf-name&gt;&gt;</code> - 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.</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Configuration Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product (config)# tcp max retries 1</td>
</tr>
</tbody>
</table>
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**

```bash
Your Product# show udp statistics vrf vrl
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:  vrl
---------
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
```
CHAPTER : UDP

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local IP Address Type</td>
<td>0</td>
</tr>
<tr>
<td>Local IP</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Local Port</td>
<td>161</td>
</tr>
<tr>
<td>Remote IP Address Type</td>
<td>0</td>
</tr>
<tr>
<td>Remote IP</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Remote Port</td>
<td>0</td>
</tr>
<tr>
<td>Local IP Address Type</td>
<td>0</td>
</tr>
<tr>
<td>Local IP</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Local Port</td>
<td>6125</td>
</tr>
<tr>
<td>Remote IP Address Type</td>
<td>0</td>
</tr>
<tr>
<td>Remote IP</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Remote Port</td>
<td>0</td>
</tr>
<tr>
<td>Local IP Address Type</td>
<td>0</td>
</tr>
<tr>
<td>Local IP</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Local Port</td>
<td>49152</td>
</tr>
<tr>
<td>Remote IP Address Type</td>
<td>0</td>
</tr>
<tr>
<td>Remote IP</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Remote Port</td>
<td>0</td>
</tr>
</tbody>
</table>

Related Command(s)
- **show udp statistics** - Displays the udp statistics.
Chapter 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 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

---

Supermicro Switch Configuration CLI Guide

CHAPTER : L2 DHCP SNOOPING

407
14.3 **ip dhcp snooping - VLAN Interface Command**

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>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.</th>
</tr>
</thead>
</table>
| 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. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td>ip dhcp snooping trust</td>
</tr>
<tr>
<td></td>
<td>no ip dhcp snooping trust</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Interface Configuration mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>Ports are considered as trusted</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product (config-if)# ip dhcp snooping trust</td>
</tr>
</tbody>
</table>
14.5 show ip dhcp snooping globals

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the global configuration of DHCP snooping. The global status of layer 2 DHCP snooping and MAC verification are displayed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>show ip dhcp snooping globals [switch &lt;Context Name&gt;]</td>
</tr>
<tr>
<td>Parameter Description</td>
<td>• switch&lt;Context Name&gt; - 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.</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# show ip dhcp snooping globals</td>
</tr>
<tr>
<td></td>
<td>DHCP Snooping Global information</td>
</tr>
<tr>
<td></td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Layer 2 DHCP Snooping is globally disabled</td>
</tr>
<tr>
<td></td>
<td>MAC Address verification is enabled</td>
</tr>
<tr>
<td>Related Command(s)</td>
<td>• ip dhcp snooping - Global command - Globally enables the layer 2 DHCP snooping in the switch and allocates the resources for the DHCP snooping module.</td>
</tr>
<tr>
<td></td>
<td>• ip dhcp snooping verify mac-address - Globally enables DHCP MAC verification in the switch.</td>
</tr>
</tbody>
</table>
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
```
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 3
30.0.0.4 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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command adds a static IP source binding entry. The no form of the command deletes the static IP source binding entry.</th>
</tr>
</thead>
</table>

### Syntax

```plaintext
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 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>` - 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

<table>
<thead>
<tr>
<th><strong>Command Objective</strong></th>
<th>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’.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td>ip verify source [ port-security ]</td>
</tr>
<tr>
<td></td>
<td>no ip verify source [ port-security ]</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Interface Configuration Mode</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>Disable</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Your Product (config-if)# ip verify source port-security</td>
</tr>
<tr>
<td><strong>Related Command(s)</strong></td>
<td>* show ip verify source - Displays the IP source guard interface status.</td>
</tr>
</tbody>
</table>
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> ]
```

<table>
<thead>
<tr>
<th>Parameter Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>Displays the IP address of the host for which the binding information should be configured.</td>
</tr>
<tr>
<td>&lt;mac-address&gt;</td>
<td>Displays the unicast MAC address of the host for which the binding information should be configured.</td>
</tr>
<tr>
<td>dhcp-snooping</td>
<td>Displays the dynamic IP binding updation through DHCP snooping.</td>
</tr>
<tr>
<td>static</td>
<td>Displays the static ip binding configuration.</td>
</tr>
<tr>
<td>&lt;interface-type&gt;</td>
<td>Displays the type of interface to which the host is connected. The interface can be:</td>
</tr>
<tr>
<td></td>
<td>- qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.</td>
</tr>
<tr>
<td></td>
<td>- gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</td>
</tr>
<tr>
<td></td>
<td>- extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</td>
</tr>
<tr>
<td></td>
<td>- port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.</td>
</tr>
<tr>
<td>&lt;interface-id&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>vlan &lt;vlan-id (1-4094)&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>switch &lt;switch_name&gt;</td>
<td>Displays the status of the ip source binding of the specified switch.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command Objective</th>
<th>This command displays the global or VLAN statistics information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`show ip binding counters [[vlan &lt;short (1-4094)&gt;]</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td><code>vlan &lt;short (1-4094)&gt;</code> - 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.</td>
</tr>
<tr>
<td></td>
<td><code>global</code> - Displays the static information of all binding types (static, dhcp, ppp)</td>
</tr>
<tr>
<td></td>
<td><code>switch &lt;switch-name&gt;</code> - Displays the static information of the specified VLAN.</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC Mode</td>
</tr>
<tr>
<td>Example</td>
<td>Your Product# show ip binding counters vlan 2</td>
</tr>
</tbody>
</table>

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 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>` – 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
```
### Supermicro Switch Configuration CLI Guide

<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/12</td>
<td>Disable</td>
</tr>
<tr>
<td>Gi0/13</td>
<td>Disable</td>
</tr>
<tr>
<td>Gi0/14</td>
<td>Disable</td>
</tr>
<tr>
<td>Gi0/15</td>
<td>Disable</td>
</tr>
<tr>
<td>Gi0/16</td>
<td>Disable</td>
</tr>
<tr>
<td>Gi0/17</td>
<td>Disable</td>
</tr>
<tr>
<td>Gi0/18</td>
<td>Disable</td>
</tr>
<tr>
<td>Gi0/19</td>
<td>Disable</td>
</tr>
<tr>
<td>Gi0/20</td>
<td>Disable</td>
</tr>
<tr>
<td>Gi0/21</td>
<td>Disable</td>
</tr>
<tr>
<td>Gi0/22</td>
<td>Disable</td>
</tr>
<tr>
<td>Gi0/23</td>
<td>Disable</td>
</tr>
<tr>
<td>Gi0/24</td>
<td>Disable</td>
</tr>
</tbody>
</table>

**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
```