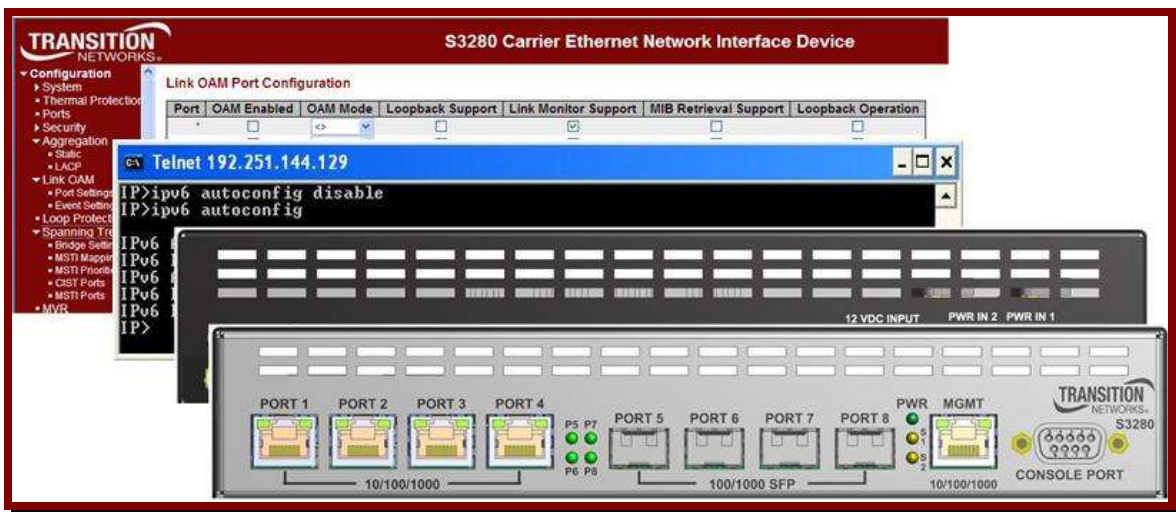




S3280 Family of Carrier Ethernet Network Interface Devices (NIDs)



CLI Reference

33507 Rev. F

Trademarks

All trademarks and registered trademarks are the property of their respective owners.

Copyright Notice/Restrictions

Copyright© 2011, 2012, 2013 Transition Networks
All rights reserved.

No part of this work may be reproduced or used in any form or by any means (graphic, electronic or mechanical) without written permission from Transition Networks.

Printed in the U.S.A.

S3280 Family of Carrier Ethernet NIDs CLI Reference Guide, 33507 Rev. F

Contact Information

Transition Networks
10900 Red Circle Drive
Minnetonka, MN 55343 USA
Tel: 952-941-7600 or 1-800-526-9267
Fax: 952-941-2322

Revision History

Rev	Date	Description
A	02/28/12	Software Version S3280 (standalone) v 1.0.2 / Software Date 2012-02-10.
B	08/24/12	Updated for Software v1.2.3. Change 'ECE Outer Tag Mode' to 'NNI-to-UNI Tag Mode'. Add MGMT Port to MAC table. Update with L2 BWP change, L2CP behaviors, and MIB/trap information.
C	12/05/12	Add S3280-TST, FW v 1.3.9 and FPGA v 1.1. Add System PowerSupply Active/Present. Increase MGMT Port MaxFrame size to tagged frame length. Add EtherSAT Loopback commands. Add "Firmware Peripheral" commands. Add "ptp oneppsaction" and "ptp extclockmode" commands. Update "loop protect port action" command. Change SSH RSA hostkey length to 2048 bits. Change name of ET-FPGA firmware .dat file.
D	01/21/12	Updated for Software v1.4. Add RFC2544 support, thermal protect trap, and add MIBs. Change SSH RSA hostkey length to 2048 bits.
E	06/11/13	Updated for Software v 1.5 (2.5GB SFP ports support, Static IP Routing, and BWP per CoS/per EVC/per UNI option. Change "Symbol frame period error events" default value. Change the LOAM v2 trap OID length. Add the MEP ID to the SOAM trap.
F	08/30/13	Updated for Software v 1.6. Adds EVC Policy ID attribute, QoS order feature.

Contents

Introduction	5
Models.....	5
Related Documents	5
Documentation Conventions.....	6
Command Line Editing.....	7
COM Port Set-up.....	9
Login	9
Navigation	10
CLI Command Groups	11
General Commands.....	11
System Commands	14
Configuration Management Commands.....	24
IP Commands.....	26
Port Commands.....	35
MAC Commands	51
VLAN Management Port (MPort) PortType Command	56
VLAN Commands	57
PVLAN Commands.....	73
Security Commands	76
STP Commands	159
Aggr (Aggregation) Commands.....	175
LACP Commands.....	179
LLDP Commands	185
EVC Commands	195
EPS Commands	212
MEP Commands.....	219
QoS Commands	233
Mirror Commands.....	259
Firmware Commands	261
PTP Commands	271
MVR Commands	288
ERPS Commands.....	298
LOAM Commands	307
Loop Protect Commands.....	321
IPMC Commands	328
sFlow Commands	344
VCL Commands	348
EtherSAT Loopback Configuration Commands (S3280-TST Only)	355
Static Routing (SIR) Commands (S3280-TST Only).....	355
Troubleshooting.....	356
Messages and Recovery.....	356
Basic Recovery Steps.....	356
CLI Messages	357
System Log Messages.....	383
Info Level Messages.....	383
Warning Level Messages	383
Error Level Messages.....	384
Third Party Program Messages	385
Recording Model and System Information	388
Technical Support	390
S3280 CLI Command Summary by Group	391
Command Groups.....	391
General Commands.....	392
System Commands.....	392
Config Commands	392

Loop Protect Commands	392
IP Commands	392
Port Commands	393
MAC Commands.....	393
VLAN Commands	393
PVLAN Commands.....	394
Security Commands.....	394
STP Commands.....	397
Aggr Commands	397
LACP Commands	398
LLDP Commands.....	398
Thermal Commands	398
EVC Commands	398
EPS Commands.....	399
MEP Commands.....	399
QoS Commands.....	399
Mirror Commands	400
Firmware Commands.....	401
MVR Commands.....	401
PTP Commands.....	401
ERPS Commands.....	402
LOAM Commands.....	402
IPMC Commands.....	402
sFlow Commands	403
VCL Commands.....	403
EtherSAT Loopback Commands	403
Static Routing (SIR) Commands.....	403
Alphabetical List of S3280 CLI Commands.....	404
A	404
C.....	404
E.....	404
F.....	405
H.....	405
I.....	405
L.....	406
M.....	407
P.....	408
Q.....	408
S.....	410
T.....	413
U.....	413
V.....	414
S3280 CLI Commands with Privilege Levels	415
Index.....	426

Figures

Figure 1: S3280 CLI Welcome Screen.....	9
Figure 2a: S3280 CLI Commands Screen	9
Figure 2b: S3280-TST CLI Commands Screen	10

Tables

Table 1: Documentation Conventions	6
Table 2: Keystroke Editing Commands.....	8
Table 3. Syslog Info Messages	383
Table 4. Syslog Warning Messages.....	384
Table 5. Syslog Error Messages	384

Introduction

The S3280 family offers a rich set of commands through its CLI for performing configuration and status monitoring. The CLI is accessible through the RS-232 serial console, telnet and SSH. The CLI incorporates user authentication for security purposes.

The CLI interface can be accessed via Secure Shell (SSH) interface. This provides a more secure interface as SSH uses public-key cryptography for authentication. When the SSH server is enabled, normal telnet access can be enabled or disabled to avoid potential security holes.

This manual is for experienced network administrators who are responsible for configuring and maintaining the S3280. The CLI offers a comprehensive set of management features for use during initial setup (set IPs etc.) and troubleshooting, as well as for day-to-day management (device management, firmware upgrades, managing security features, etc.). This manual is for use following a successful install per the applicable S3280 Install Guide manual.

Note: CLI commands are case sensitive. Enter the CLI commands in lower case unless otherwise specified. In order to execute the commands described in this manual, you must press Enter after the command has been entered.

Models

The S3280 NID models are listed below. This manual documents the following models and specifies where differences between models exist.

Model	Description
S3280	Base S3280 NID.
S3280-TST	Base S3280 with wire speed loopback and RFC 2544 test generation.

Note that references to “S3280” in this manual relate to the above models, unless otherwise specified.

Related Documents

The S3280 documentation set includes:

- Product Documentation Postcard, 33504
- S3280 Install Guide (33513) or S3280-TST Install Guide, 33520
- S3280 Web Interface User Guide, 33506
- S3280 Command Line Interface (CLI) User Guide, 33507 (this manual)
- Converge™ EMS Admin Guide 33533, Install Guide 33543, Admin Procedures 33544
- RFC2544 User Guide, 33540
- Static IP Routing User Guide, 33542
- Release Notes (version specific)

Check the TN web site at www.transition.com for additional white papers, application notes, etc.

Documentation Conventions

The conventions used within this manual for commands/input entries are described in the table below.

Table 1: Documentation Conventions

Convention	Meaning
Boldface text	Indicates the entry must be made as shown. For example: ipaddr=<addr> In the above, only ipaddr= must be entered exactly as you see it, including the equal sign (=).
< >	Arrow brackets indicate a value that must be supplied by you. Do not enter the symbols < >. For example: ipaddr=<addr> In place of <addr> you must enter a valid IP address.
[]	Indicates an optional keyword or parameter. For example: go [s=<xx>] In the above, go must be entered, but s= does not have to be.
{ }	Indicates that a choice must be made between the items shown in the braces. The choices are separated by the symbol. For example: state={enable disable} Enter state=enable or state=disable .
“ ”	Indicates that the parameter must be entered in quotes. For example: time=<“value”> Enter time=“20100115 13:15:00” .
>	Indicates a selection string. For example: Select File>Save . This means to first select/click File then select/click Save .


The S3280 CLI is compatible with several terminal emulators: Absolute Telnet, HT, HTPe, Java Hyper Terminal, PuTTY, SecureCRT, TeraTermPro (open source), Windows Phone & Modem options, and Windows Remote Shell (CLI). Telnet clients: Absolute Telnet, Microsoft Telnet Client, PuTTY, TeraTerm, Van Dyke SecureCRT, ZOC, Zephyr Passport, and Zugg TeSSH. Tftp servers: Tftpd32 and Tftpd64, SolarWinds TftpServer, etc. Syslog servers: Tftpd32 and Tftpd64, SolarWinds LogForwarder, Kiwi Syslog, Server, etc.


Command Line Editing

This section describes how to enter CLI commands.

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters.

Display Similar Commands

At the command line, you can use the keyboard  key or **?** key to show available commands in a category of commands after entering a part of the command.

For example, use the  key to enter part of the command to display all of the available commands that start with **show ether**. The commands display in a single row.

Use the **?** key after a partial CLI command entry to display all of the available commands that start with **show ether**, but in a single column:

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember to not leave a space between the command and question mark.) For example “**s?**” shows all the keywords starting with “s.”

Recall Commands

To recall recently-entered commands from the command history, perform one of the optional actions below:

Ctrl-P or **Up arrow** (↑) key: Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.

Ctrl-N or **Down arrow** (↓) key: Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up arrow key. Repeat the key sequence to recall successively more recent commands.

Keystroke Commands

The table below shows the optional keystrokes available to edit command lines (* indicates HyperTerminal support, ** indicates command prompt support, *** indicates both HyperTerminal and command prompt support by this keystroke).

Table 2: Keystroke Editing Commands

Capability	Keystroke	Purpose
Move the command line around to make changes or corrections	Ctrl-B *** or left (←) arrow key ***	Move the cursor back one character
	Ctrl-F *** or right (→) arrow key ***	Move the cursor forward one character
	Ctrl-A ***	Move the cursor to the beginning of the command line
	Ctrl-E ***	Move the cursor to the end of the command line
Recall commands from the buffer and paste them in the command line	Ctrl-Y ***	Recall the most recent entry in the buffer
	Ctrl-T **	Transpose the character to the left of the cursor with the character located at the cursor
	Ctrl-Y **	Recall the most recent entry in the buffer
Delete entries (if you make a mistake or change your mind)	Delete key *** or Backspace key ***	Erase the character to the left of the cursor
	Ctrl-D ***	Delete the character at the cursor
	Ctrl-K ***	Delete all characters from the cursor to the end of the command line
	Ctrl-U *** or Ctrl-X ***	Delete all characters from the cursor to the beginning of the command line
	Ctrl-W ***	Delete the word to the left of the cursor
	Esc D **	Delete from the cursor to the end of the word
Capitalize or lowercase words or capitalize a set of letters	Esc C *	Change case from capital to lower-case (or lower-case to capital) at the cursor
Redisplay the current command line if the switch unexpectedly sends a message to your screen	Ctrl-L *** or Ctrl-R ***	Redisplay the current command line (reverse-i-search)

COM Port Set-up

To use the CLI, connect a PC COM port to the RS232 connector and activate a terminal emulation program (e.g., HyperTerminal under Windows). The COM port must be set at 8 data bits, 1 stop bit, no parity, 115200 baud and no flow control.

Login

Enter CLI command mode via telnet, HyperTerminal, etc. Enter the default Username **admin** and then hit **Enter** twice to enter CLI command mode (no default Password). The following information displays.

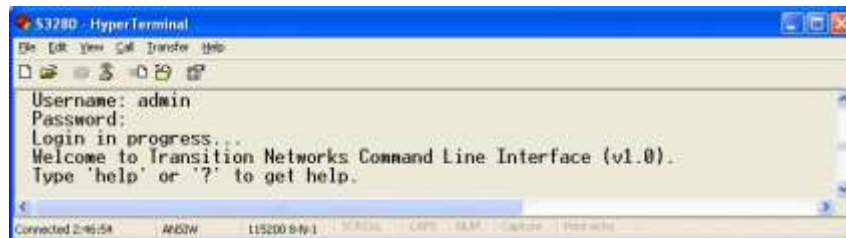


Figure 1: S3280 CLI Welcome Screen

At the > prompt, type ? (or type **Help**) and press **Enter** to display the CLI help screen as shown below.

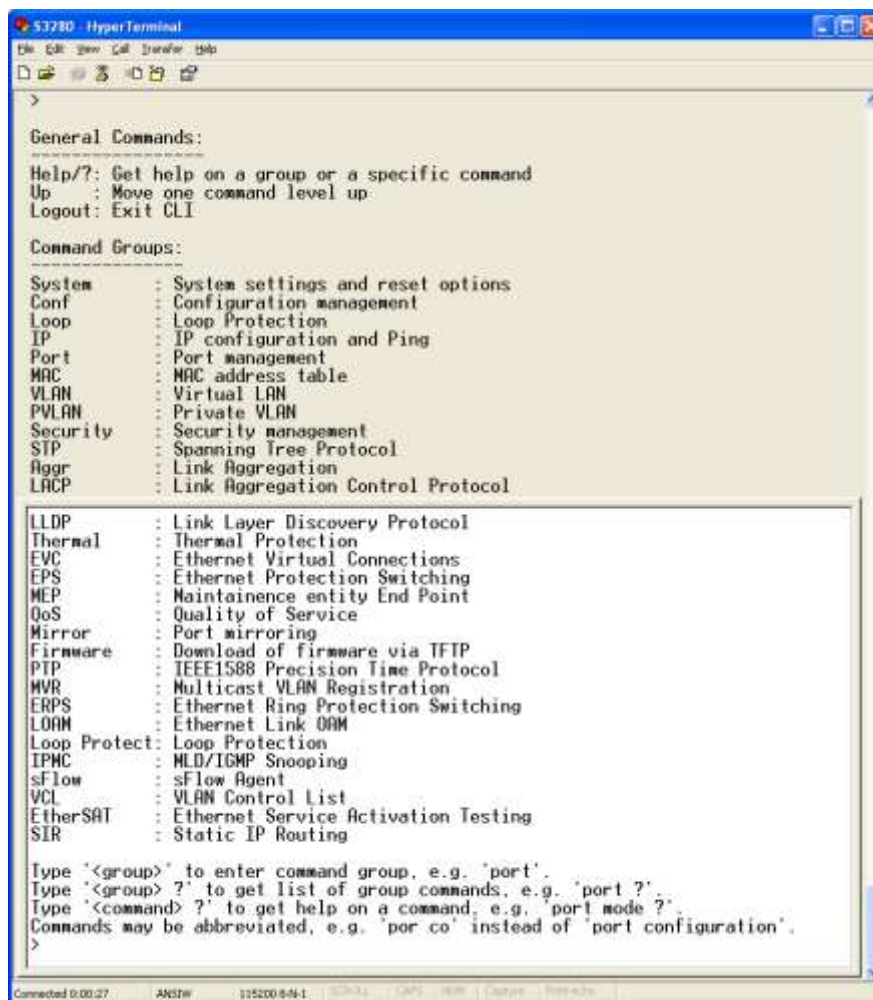
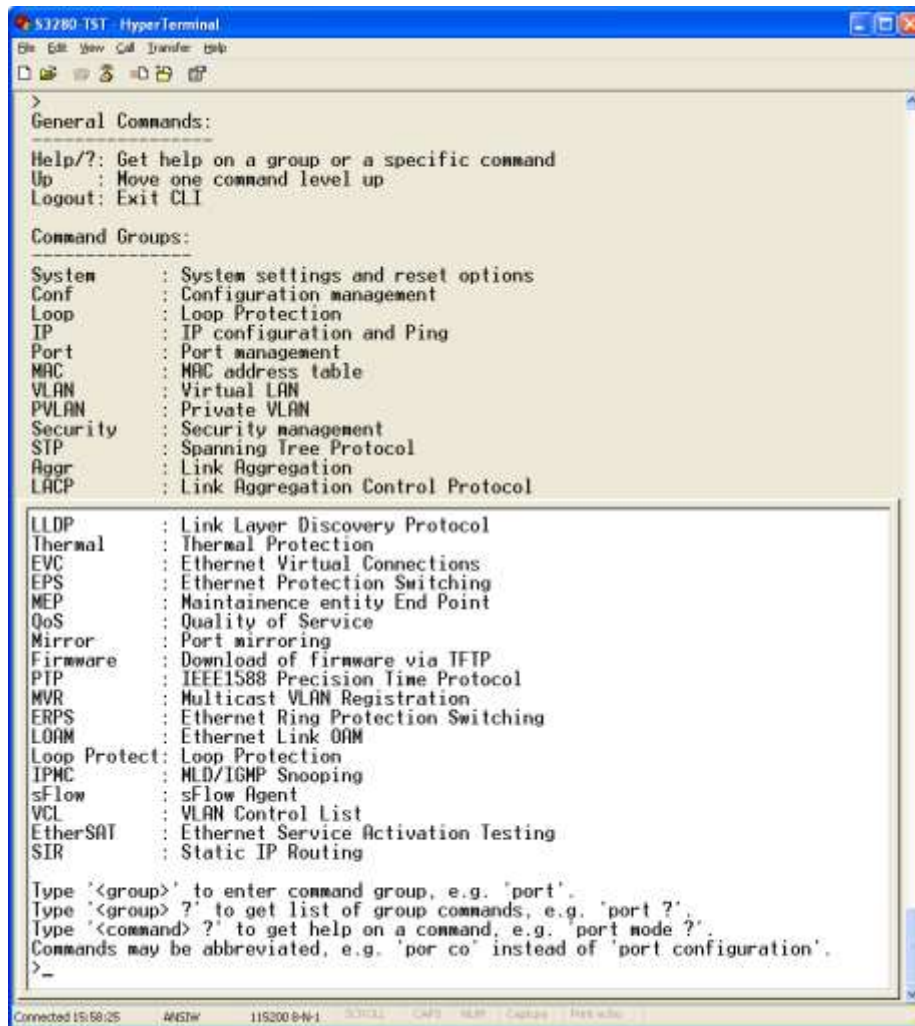


Figure 2a: S3280 CLI Commands Screen



```

S3280-TST - HyperTerminal
File Edit View Call Transfer Help
[Icons]
>
General Commands:
-----
Help/? : Get help on a group or a specific command
Up      : Move one command level up
Logout : Exit CLI

Command Groups:
-----
System      : System settings and reset options
Conf        : Configuration management
Loop        : Loop Protection
IP          : IP configuration and Ping
Port        : Port management
MAC         : MAC address table
VLAN        : Virtual LAN
PVLAN       : Private VLAN
Security    : Security management
STP         : Spanning Tree Protocol
Aggr        : Link Aggregation
LACP        : Link Aggregation Control Protocol

LLDP        : Link Layer Discovery Protocol
Thermal     : Thermal Protection
EVC         : Ethernet Virtual Connections
EPS         : Ethernet Protection Switching
MEP         : Maintenance entity End Point
QoS         : Quality of Service
Mirror      : Port mirroring
Firmware    : Download of firmware via TFTP
PTP         : IEEE1588 Precision Time Protocol
MVR         : Multicast VLAN Registration
ERPS       : Ethernet Ring Protection Switching
LOAM        : Ethernet Link OAM
Loop Protect : Loop Protection
IPMC        : NLD/IGMP Snooping
sFlow       : sFlow Agent
VCL         : VLAN Control List
EtherSAT    : Ethernet Service Activation Testing
SIR         : Static IP Routing

Type '<group>' to enter command group, e.g. 'port'.
Type '<group> ?' to get list of group commands, e.g. 'port ?'.
Type '<command> ?' to get help on a command, e.g. 'port mode ?'.
Commands may be abbreviated, e.g. 'por co' instead of 'port configuration'.
>

```

Figure 2b: S3280-TST CLI Commands Screen

Navigation

Type '**<group>**' to enter a command group (e.g., '**port**' group of commands).

Type '**<group>**' to get a list of group commands (e.g., '**port ?**' group, with a space between 'port' and the ?).

Type '**<command> ?**' to get help on a command (e.g., '**port mode ?**').

Commands may be abbreviated (e.g., '**po co**' instead of 'port configuration').

CLI syntax is case-independent (command entry is not case sensitive).

All of the CLI command groups and the individual commands are discussed in the following sections.

CLI Command Groups

The commands are grouped based on functions, and offer submenus that are context sensitive (e.g., all ‘VLAN’ commands are accessible using the ‘vlan’ keyword or by entering the ‘vlan’ submenu).

The S3280 supports 30 command groups which include a total of over 500 commands. The S3280-TST supports several additional commands. Note that certain features (RFC 2544, and Static IP Routing) have separate manuals each with its own Web GUI and CLI descriptions and procedures. See “[Related Documents](#)” on page 5 of this manual.

General Commands

The General commands include **Help**, **Up**, **/** (go to root), and **Logout**. The General commands in Telnet are shown below.

```
General Commands:
-----
Help/? : Get help on a group or a specific command
Up     : Move one command level up
Logout: Exit CLI
```

The General commands in HyperTerminal are shown below.

```
General Commands:
-----
Help/? : Get help on a group or a specific command
Up     : Move one command level up
Logout: Exit CLI
```

The General commands (Help, Up, /, and Logout) are explained below.

Command: / (Go to root level)

Syntax: /

Description: Type / (slash character) to go to the CLI root level in the CLI command structure.

Example:

```
>system
Type 'up' to move up one level or '/' to go to root level
System>/
>
```

Command: **Help** or **?**

Syntax: **help** <cr> or **?**<cr>

Description: Get assistance (help) on a group of commands or on a specific command.

Example:

```
>help
General Commands:
-----
Help/?: Get help on a group or a specific command
Up      : Move one command level up
Logout: Exit CLI

Command Groups:
-----
System      : System settings and reset options
Conf        : Configuration management
Loop        : Loop Protection
IP          : IP configuration and Ping
Port        : Port management
MAC         : MAC address table
VLAN        : Virtual LAN
PVLAN       : Private VLAN
Security    : Security management
STP         : Spanning Tree Protocol
Aggr        : Link Aggregation
LACP        : Link Aggregation Control Protocol
LLDP        : Link Layer Discovery Protocol
Thermal     : Thermal Protection
EVC         : Ethernet Virtual Connections
EPS         : Ethernet Protection Switching
MEP         : Maintenance entity End Point
QoS         : Quality of Service
Mirror      : Port mirroring
Firmware    : Download of firmware via TFTP
PTP         : IEEE1588 Precision Time Protocol
MVR         : Multicast VLAN Registration
ERPS        : Ethernet Ring Protection Switching
LOAM        : Ethernet Link OAM
Loop Protect: Loop Protection
IPMC        : MLD/IGMP Snooping
sFlow       : sFlow Agent
VCL         : VLAN Control List
EtherSAT    : Ethernet Service Activation Testing
SIR         : Static IP Routing

Type '<group>' to enter command group, e.g. 'port'.
Type '<group> ?' to get list of group commands, e.g. 'port ?'.
Type '<command> ?' to get help on a command, e.g. 'port mode ?'.
Commands may be abbreviated, e.g. 'por co' instead of 'port configuration'.
>
```

Note: The S32880-TST models have **EtherSAT** Loopback commands and Firmware Peripheral commands that the S3280 does not support.

Command: Up

Syntax: up

Description: Move one command level up (e.g., from group level to root level).

Example:

```
>system
Type 'up' to move up one level or '/' to go to root level
System>up
>system
Type 'up' to move up one level or '/' to go to root level
System>/
>
```

Command: Logout

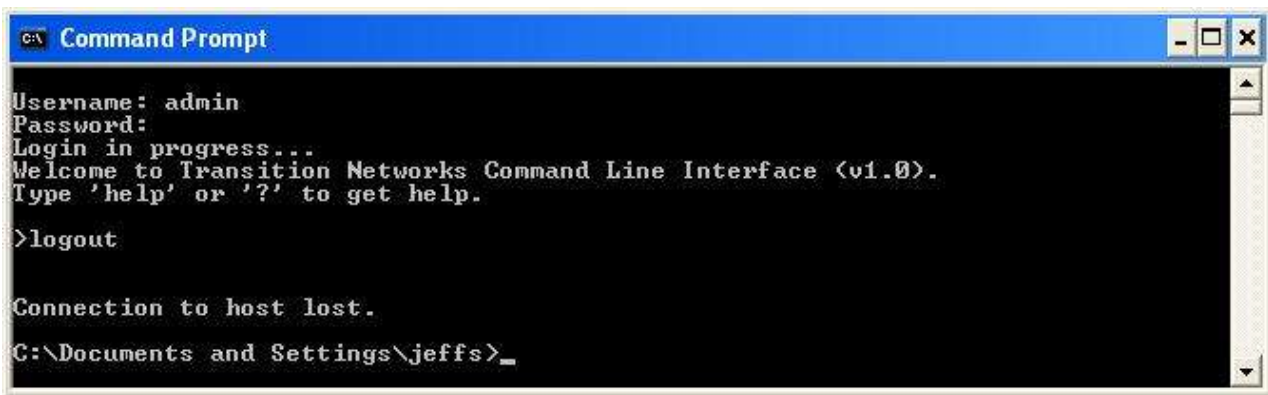
Syntax: logout

Description: Exit the CLI. The telnet or HyperTerminal connection is dropped. You must log back in after entering the **logout** command.

Example:

```
>logout
>
Username:
```

Example: Telnet:



```

C:\ Command Prompt
Username: admin
Password:
Login in progress...
Welcome to Transition Networks Command Line Interface (v1.0).
Type 'help' or '?' to get help.

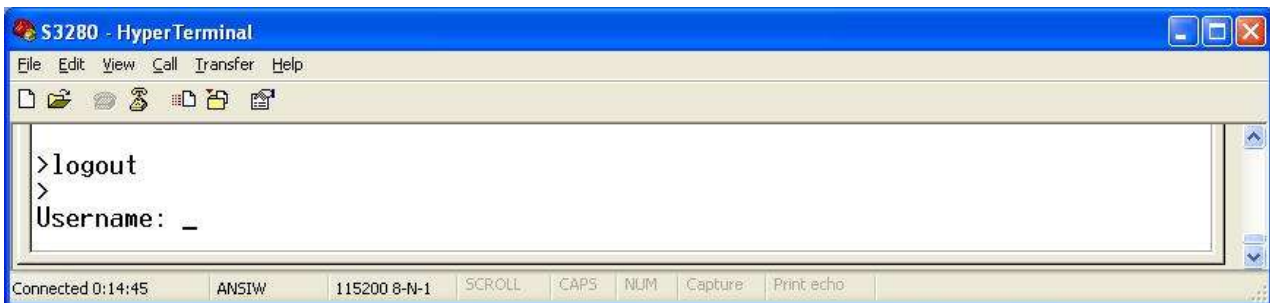
>logout

Connection to host lost.

C:\Documents and Settings\jeffs>_

```

HyperTerminal:



```

S3280 - HyperTerminal
File Edit View Call Transfer Help
[Icons]
>logout
>
Username: _

```

Connected 0:14:45 ANSIW 115200 8-N-1 SCROLL CAPS NUM Capture Print echo

System Commands

These ‘System’ group commands provide S3280 settings and reset options:

```
>system ?
Available Commands:

System Configuration [all | (port <port_list>)]
System Log Configuration
System Timezone Configuration
System Version
System Log Server Mode [enable|disable]
System Name [<name>]
System Timezone Offset [<offset>]
System Contact [<contact>]
System Log Server Address [<ip_addr_string>]
System Timezone Acronym [<acronym>]
System DST Configuration
System Location [<location>]
System Log Level [info|warning|error]
System DST Mode [disable|recurring|non-recurring]
System DST start <week> <day> <month> <date> <year> <hour> <minute>
System Log Lookup [<log_id>] [all|info|warning|error]
System DST end <week> <day> <month> <date> <year> <hour> <minute>
System Log Clear [all|info|warning|error]
System Reboot
System Date
System DST Offset [<dst_offset>]
System PowerSupply Active
System Load
>
```

The S3280 ‘System’ group of commands are explained below.

Command: Show System Configuration

Syntax: **system configuration** [all | (port <port_list>)]

Description: Displays all of the current S3280 or S3280-TST operating parameters. The default is “Show (basic) system configuration”. The parameters are:

- all** : Show all switch configuration (this is a long display if you include the “all” keyword).
- port** : Show switch port configuration.
- <port_list>**: Port list or 'All'. The default is ‘All’ ports.

```
Example 1: >sys config
System Contact :
System Name :
System Location :
MAC Address : 00-c0-f2-21-db-83
Software ID : S3280
Product ID : S3280
Serial # : 12094402
Board Rev : 4
FPGA Version : v2.1
Chip ID : VSC7428 Rev. B
System Time : 1970-01-01T00:32:37+00:00
System Uptime : 00:32:37
Software Version: S3280 (standalone) 1.6.4
Software Date : 2013-08-28T16:02:41-05:00
Previous Restart: Cool
>
```

Command: Show System Log Configuration

Syntax: system log configuration

Description: Displays the current system log configuration (mode, address, and level).

Example: >sys log config

```
System Log Configuration:
=====
System Log Server Mode      : Enabled
System Log Server Address  : 192.168.1.110
System Log Level           : Warning
>
```

Command: Show System Version

Syntax: system version

Description: Displays the current S3280 or S3280-TST software version information.

Example 1: >sys ver

```
Version      : S3280 (standalone) 1.6.4
Build Date   : 2013-08-28T16:02:41-05:00
>
```

Command: **System Name**

Syntax: **system name** [<name>] [clear]

Description: Set, clear, or show the S3280 system name, where:

<name>: System name string. (1-255).

Use "" (opening and closing quote characters) to clear the string.

System name is a text string using the alphabet (A-Z, a-z), digits (0-9), minus sign (-) characters. In CLI, no blank or space characters are permitted as part of a system name.

The first character must be an alpha character, and the first or last character must not be a minus sign. Setting a system name will add the new name in front of the > command prompt. Any entry with an _ (underscore) character is ignored.

"" : Clear the current system name entry.

```
Example: >system name DevSys2
System Name      : DevSys2
DevSys2:/>/
DevSys2:/>sys name ""
DevSys2:/>system name
System Name      :
>system name DevSys2
>system name
System Name      : DevSys2
DevSys2:/>system name clear
DevSys2:/>system name
System Name      : clear
clear:/>
```

Note: you can not access S3280 by system name via DHCP/DNS.

Command: **System Contact**

Syntax: **System Contact** [<contact>] [clear]

Description: Set, clear, or show the system contact, where:

<contact>: System contact string. (1-255). Use "" (opening and closing quote characters) to clear the string. In CLI, no blank or space characters are permitted as part of a contact unless enclosed in double quotes..

"" : Clear the system contact entry.

```
Example: >system contact
System Contact   : RJ-Stylesh-dev1
>system contact clear
>system contact
System Contact   : clear
>system contact "
Invalid parameter: "

Syntax:
System Contact [<contact>]
>system contact ""
>system contact
System Contact   :
>sys contact "__ __"
>sys contact
System Contact   : __ __
>
```


Command: **System Log Server Address**

Syntax: **system log server address** [<ip_addr_string>]

Description: Show or set the system log server address, where:
<ip_addr_string>: IP host address (a.b.c.d).

Example:

```
>system log server address 192.168.1.30
>system log server address
System Log Server Address : 192.168.1.30
>
```

Command: **System Location**

Syntax: **system location** [<location>] [clear]

Description: Set, clear, or show the system location, where:
<location>: System location string. (1-255). Use "" (double quotes) to clear the string. In CLI, no blank or space characters are permitted as part of a location unless enclosed in double quotes.
"": Clear the current system location entry.

Example:

```
>system location
System Location :
>system location 10900_Red_CircleDrive
>system location clear
>system location
System Location : clear
>system location ""
>system location
System Location :
>
```

Command: **System Log Configuration**

Syntax: **system log config**

Description: Show system log configuration.

Example: **system log config**

```
System Log Configuration:
=====
System Log Server Mode      : Enabled
System Log Server Address  : 192.168.1.30
System Log Level           : Warning
>
```

Command: **Enable / Disable System Log Server Mode**

Syntax: **system log server mode** [enable|disable]

Description: Show or set the system log server mode, where:
enable : Enable system log server mode.
disable: Disable system log server mode.
(The default is Show system Log server mode.)

Example:

```
>System Log Server Mode
System Log Server Mode      : Enabled
>System Log Server Mode disable
>System Log Server Mode
System Log Server Mode      : Disabled
>
```

Command: **System Log Level**

Syntax: **system log level** [info|warning|error]

Description: Show or set the system log level. Set defines the kind of message to be sent to a third party syslog server, where:

info : Send informations, warnings, and errors.

warning : Send just warnings and errors.

error : Send errors only.

all: send all three levels of syslog messages (info, warning ,and error).

Example:

```
>system log level info
>system log level
System Log Level           : Info
>
```

Command: **Clear System Log**

Syntax: **system log clear** [all|info|warning|error]

Description: Clear all or portions of the system log, where:

all : Clear all levels (the default).

info : Clear just the information (INFO) log entries.

warning : Clear just the warning (WARN) log entries.

error : Clear just the error (ERROR) log entries.

Example:

```
>sys log lookup
Number of entries:
Info      : 4
Warning: 0
Error    : 0
All      : 4

ID      Level   Time                               Message
-----  -
  1  Info   1970-01-01T00:00:00+00:00   Switch just made a cold boot.
  2  Info   1970-01-01T00:00:02+00:00   Using primary power source.
  3  Info   1970-01-01T00:00:05+00:00   Link up on port 1
  4  Info   1970-01-01T00:00:06+00:00   Link up on port 5
>sys log clear
>sys log lookup
>
```

Command: System Log Lookup**Syntax:** `system log lookup` [<log_id>] [all|info|warning|error] [clear]**Description:** Show or clear the system log. See “[System Log Messages](#)” on page 383 for the full set of System Log message descriptions. The parameters are:

<log_id>: System log ID or range (default: All entries)

all : Show all levels (default)**info** : Show informational level messages only.**warning** : Show warning level messages only.**error** : Show error level messages only.**clear** : Clear the system log.

Example:

```
>system log lookup 1
ID      : 1
Level   : Info
Time    : -
Message:

Switch just made a cool boot.
```

Example:

```
>system log lookup
Number of entries:
Info      : 7
Warning: 0
Error    : 5
All      : 12

ID      Level   Time                               Message
-----  -
1      Info    -   Switch just made a cool boot.
2      Info    1970-01-01T00:00:02+00:00   Link up on port 6
3      Info    1970-01-01T00:00:02+00:00   Using primary power source.
4      Info    1970-01-01T00:00:07+00:00   Link up on port 3
5      Error   1970-01-01T00:26:54+00:00   VLAN Port Configuration Ingress Fil ...

6      Error   1970-01-01T00:26:54+00:00   VLAN Port Configuration Ingress Fil ...

7      Error   1970-01-01T00:26:54+00:00   VLAN Port Configuration Ingress Fil ...

8      Error   1970-01-01T00:26:54+00:00   VLAN Port Configuration Ingress Fil ...

9      Info    1970-01-01T03:31:43+00:00   Link down on port 6
10     Info    1970-01-04T01:15:48+00:00   Link down on port 3
11     Info    1970-01-04T01:15:54+00:00   Link up on port 3
12     Error   1970-01-04T01:15:54+00:00   VLAN Port Configuration Ingress Fil ...

>
```

Command: Display System Timezone Configuration
Syntax: system timezone config
Description: Display the current system Timezone configuration.
Example: >system timezone config

```
System Timezone Configuration:
=====
Timezone Offset : 0 ( 0 minutes)
>
```

Command: System Timezone Offset
Syntax: system Timezone Offset [<offset>]
Description: Set or show the system timezone offset, where:
 <offset>: Time zone offset in minutes (-7200 to 7201) relative to UTC.

Example: >sys timezone offset
 Timezone Offset : 0 (0 minutes)
 >sys timezone offset 42
 >sys timezone offset
 Timezone Offset : 42 (4 minutes)
 >

Command: System Timezone Acronym
Syntax: system timezone acronym [<acronym>]
Description: Set or show the system timezone acronym, where:
 <acronym>: Time zone acronym (0 - 16 characters; the space character is not allowed).

Example: >System Timezone Acronym
 Timezone Acronym :
 >System Timezone Acronym MnDST
 >System Timezone Acronym
 Timezone Acronym : MnDST
 >

Command: System DST Mode
Syntax: system dst mode [disable|recurring|non-recurring]
Description: Set or show the daylight saving time (DST) mode, where:
disable: Disable Daylight Saving Time.
recurring: Enable Daylight Saving Time as recurring mode.
non-recurring: Enable Daylight Saving Time as non-recurring mode.

Example: >system dst mode
 Daylight Saving Time Mode : Disabled.
 >system dst mode recurring
 >system dst mode
 Daylight Saving Time Mode : Recurring.
 >system dst mode non-recurring
 >system dst mode
 Daylight Saving Time Mode : Non-Recurring.
 >

Command: Show System DST Configuration

Syntax: system dst configuration

Description: Display the current Daylight Saving Time (DST) configuration.

Example: >system dst config

```
System Daylight Saving Time(DST) Configuration:
=====

Daylight Saving Time Mode : Disabled.
Daylight Saving Time Start Time Settings :
    Week: 0
    Day: 0
    Month: 0
    Date: 0
    Year: 0
    Hour: 0
    Minute: 0
Daylight Saving Time End Time Settings :
    Week: 0
    Day: 0
    Month: 0
    Date: 0
    Year: 0
    Hour: 0
    Minute: 0
Daylight Saving Time Offset : 1 (minutes)
```

* : This symbol indicates the parameter must be set to a reasonable value.

Command: System DST Start

Syntax: system dst start <week> <day> <month> <date> <year> <hour> <minute>

Description: Set or show the daylight saving time start time settings, where:

<week> : Week (1-5), 0: ignored.

<day> : Day (1-7), 0: ignored.

<month> : Month (1-12), 0: ignored.

<date> : Date (1-31), 0: ignored.

<year> : Year (2000-2097).

<hour> : Hour (0-23).

<minute>: Minutes (0-59).

Example: >system dst start 1 2 3 4 2012 5 6
>

Messages: Missing <week> parameter

Command: System DST End**Syntax:** `system dst end <week> <day> <month> <date> <year> <hour> <minute>`**Description:** Set or show the daylight saving time end time and date settings, where:

<week> : Week (1-5), 0: ignored.
<day> : Day (1-7), 0: ignored.
<month> : Month (1-12), 0: ignored.
<date> : Date (1-31), 0: ignored.
<year> : Year (2000-2097).
<hour> : Hour (0-23).
<minute>: Minutes (0-59).

Example: `>system dst end 0 0 0 0 2012 1 1`
`>`

Messages: *Missing <week> parameter***Command: System DST Offset****Syntax:** `system dst offset [<dst_offset>]`**Description:** Set or show the daylight saving time offset, where:**<dst_offset>**: DST offset in minutes (1 to 1440).

Example: `>system dst offset`
Daylight Saving Time Offset : 1 (minutes)
`>system dst offset 5`
`>system dst offset`
Daylight Saving Time Offset : 5 (minutes)
`>`

Command: System PowerSupply Active**Syntax:** `system powersupply active`**Description:** Show which S3280-L power supply is active.

Example: `>system power`
Power Supply Active: Primary
`>`

Messages: *Device not capable of Power Supply Monitoring\n (displays on S3280-H model).*

Command: **System Reboot**
Syntax: **system reboot**
Description: Reboots (warm start) the S3280, displays a series of text data, and then displays the password prompt. You must log in to the S3280 again when the system reboot is completed.

Example: **>system reboot**
System will reboot in a few seconds
>+M25PXX : Init device with JEDEC ID 0xEF4018.
S3280 board detected (VSC7428 Rev. B).

Copyright (C) 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008,
2009
Free Software Foundation, Inc.
RedBoot is free software, covered by the eCos license, derived from
the GNU General Public License. You are welcome to change it and/or
distribute copies of it under certain conditions. Under the license
terms, RedBoot's source code and full license terms must have been
made available to you. Redboot comes with ABSOLUTELY NO WARRANTY.

Platform: VCore-III (MIPS32 24KEc) LUTON26
RAM: 0x80000000-0x88000000 [0x80020dd8-0x87fe1000 available]
FLASH: 0x40000000-0x40ffffff, 256 x 0x10000 blocks
== Executing boot script in 1.000 seconds - enter ^C to abort
RedBoot> fis load -d managed
Image loaded from 0x80040000-0x806c17f8
RedBoot> go

Messages: Username:
RedBoot(tm) bootstrap and debug environment [ROMRAM]
Non-certified release, version 1_12-TN - built 07:51:34, Jan 5 2012

Command: **System Date**
Syntax: **system date**
Description: View the current date and time. Note that this command only lets you view the date and time; use NTP for persistent setting.

Example: **>system date**
1970-01-01T02:19:55+00:00
>

Command: **System Load**
Syntax: **system load**
Description: Show current CPU load: 100ms, 1s and 10s running average (in percent, zero is idle).

Example: **>system load**
Load average(100ms, 1s, 10s): 0%, 0%, 0%
>system load
Load average(100ms, 1s, 10s): 100%, 99%, 99%
>

Configuration Management Commands

These Configuration management commands provide S3280 configuration backup, default reset, and configuration restore functions. The Configuration management commands include:

>**config ?**

Available Commands:

Config Backup Binary <hostname> <file_name>

Config Restore Binary <hostname> <file_name>

Config Default [keep_ip]

>

Note: The **config backup binary** and **config restore binary** commands do not work with SolarWinds TFTP Server version 8.2.7 (September 2005). SolarWinds TFTP Server version 10.4.0.14 works fine for S3280 binary backups and restores.

The S3280 Configuration management commands are explained below.

Command: **Restore Config to Default Settings**

Syntax: **config default** [keep_ip]

Description: Restore factory default configuration, where:

keep_ip: Keep the current IP configuration. The default is 'Restore full configuration (do not keep the current IP address)'. **Note:** If you do not include the [keep_ip] parameter, you must change the S3280 IP address via the CLI before you can access the S3280 via the web interface (GUI).

Example:

```
>config default keep_ip
>config default
>ip setup 192.168.1.110
>
```

Command: **Config Backup Binary**

Syntax: **config backup binary** <hostname> <file_name>

Description: Backup the current binary configuration to a configured and enabled TFTP server. The backup file is sent to the TFTP Server, the S3280 reboots, and the help screen displays. Parameters are:

<**hostname**> : IP Address or Hostname of the TFTP server.

<**file_name**>: Name of the S3280 config file to be backed up (must be a .bin file). The filename should only contain alpha, numeric, underscore "_" and dot "." characters.

Example:

```
>config backup binary 192.168.1.30 S3280_v1.4.1_conf.bin
>
```

Note: the TFTP server must be configured and running. if the TFTP server is not running and configured, the message "tftp client put failed: x" displays.

When the transfer successfully completes, the TFTP server displays a confirmation message such as:

Connection received from 192.168.1.110 on port 7800 [27/04 16:46:42.786]

Write request for file <S3280_v1.1.2_conf.bin>. Mode OCTET [27/04 16:46:42.786]

Using local port 2020 [27/04 16:46:42.786]

<S3280_v1.1.2_conf.bin>: rcvd 13 blks, 6348 bytes in 0 s. 0 blk resent [27/04 16:46:42.786]

Command: **Config Restore Binary**

Syntax: **config restore binary** <hostname> <file_name>

Description: Restore binary configuration from a configured and enabled TFTP server. Note that you must log in to the S3280 again when done. The parameters are:

<**hostname**> : IP Address or Hostname of the TFTP server.

<**file_name**>: Name of the S3280 config file to be restored (must be a .bin file).

Example:

```
>config restore binary 192.168.1.30 S3280_v1.4.1_conf.bin
```

```
Restore successful
```

```
System Restarting...>+M25PXX : Init device with JEDEC ID 0xEF4018.
```

```
S3280 board detected (VSC7428 Rev. B).
```

```
Copyright (C) 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009
```

```
Free Software Foundation, Inc.
```

```
RedBoot is free software, covered by the eCos license, derived from the
GNU General Public License. You are welcome to change it and/or distribute
copies of it under certain conditions. Under the license terms, RedBoot's
source code and full license terms must have been made available to you.
Redboot comes with ABSOLUTELY NO WARRANTY.
```

```
Platform: VCore-III (MIPS32 24KEc) LUTON26
```

```
RAM: 0x80000000-0x88000000 [0x80020ec8-0x87fe1000 available]
```

```
FLASH: 0x40000000-0x40ffffff, 256 x 0x10000 blocks
```

```
== Executing boot script in 1.000 seconds - enter ^C to abort
```

```
RedBoot> fis load -d managed
```

```
Image loaded from 0x80040000-0x806ee950
```

```
RedBoot> go
```

```
Username:
```

```
Messages: tftp client get failed: 8
```

```
RedBoot(tm) bootstrap and debug environment [ROMRAM]
```

```
Non-certified release, version 1_12-TN - built 13:45:10, Jan 26 2012
```

Note: the TFTP server must be configured and running. if the TFTP server is not running and configured, the message “*tftp client put failed: x*” displays.

TFTP Server Messages:

```
Connection received from 192.168.1.10 on port 7800 [02/05 09:57:50.449]
```

```
Write request for file <IND-3284cfg.bin>. Mode OCTET [02/05 09:57:50.449]
```

```
Using local port 1401 [02/05 09:57:50.449]
```

```
<IND-3284cfg.bin>: rcvd 13 blks, 6478 bytes in 0 s. 0 blk resent [02/05 09:57:50.449]
```

```
Connection received from 192.168.1.10 on port 7700 [02/05 09:58:40.449]
```

```
Read request for file <IND-3284cfg.bin>. Mode OCTET [02/05 09:58:40.449]
```

```
Using local port 1402 [02/05 09:58:40.449]
```

```
<IND-3284cfg.bin>: sent 13 blks, 6478 bytes in 0 s. 0 blk resent [02/05 09:58:40.464]
```

IP Commands

The S3280 IP (Internet Protocol) group commands provide IP configuration, ARP, DHCP, DNS, MVLAN, NTP, and Ping functions. The IP commands include:

>**ip ?**

Available Commands:

IP ARP Show

IP Configuration

IP DHCP [enable|disable]

IP Setup [<ip_addr>] [<ip_mask>] [<ip_router>]

IP Ping <ip_addr_string> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)]

IP DNS [<ip_addr>]

IP DNS_Proxy [enable|disable]

IP IPv6 AUTOCONFIG [enable|disable]

IP IPv6 Setup [<ipv6_addr>] [<ipv6_prefix>] [<ipv6_router>]

IP IPv6 State <ipv6_addr> [enable|disable]

IP IPv6 Ping6 <ipv6_addr> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)]

IP MVlan [<vid>]

IP NTP Configuration

IP NTP Mode [enable|disable]

IP NTP Server Add <server_index> <ip_addr_string>

IP NTP Server Ipv6 Add <server_index> <server_ipv6>

IP NTP Server Delete <server_index>

>

Command: **IP ARP Show**

Syntax: **ip arp show**

Description: Display the current ARP (Address Resolution Protocol) configuration.

Example 1: >**ip arp show**

```
ARP Table:

0 entries in total
>
```

Example 2: >**ip arp show**

```
ARP Table:

192.168.1.30      (incomplete) on eth0

1 entries in total
>
```

Example 3: >**ip arp show**

```
ARP Table:

192.168.1.30      00:04:75:bd:9c:36 on eth0
192.168.1.110    00:c0:f2:56:08:b0 on eth0

2 entries in total
>
```

Command: Show Current IP Configuration

Syntax: ip config

Description: Displays the current S3280 IP configuration (DHCP Client state, IP address / mask, IP Router address, VLAN ID, and IPv6) information.

Example: >ip config

```
IP Configuration:
=====

DHCP Client      : Enabled
IP Address       : 192.168.1.110
IP Mask          : 255.255.255.0
IP Router        : 0.0.0.0
DNS Server       : 0.0.0.0
VLAN ID          : 1
DNS Proxy        : Disabled

IPv6 AUTOCONFIG mode : Enabled (Fallback in 300 seconds)
IPv6 Link-Local Address: fe80::2c0:f2ff:fe21:b8c4
IPv6 Address      : ::192.0.2.1
IPv6 Prefix       : 96
IPv6 Router       : ::

Active Configuration: (Static)
IP Address        : 192.168.1.110
IP Mask           : 255.255.255.0
IP Router         : 0.0.0.0
DNS Server        : 0.0.0.0

Active Configuration for IPv6: (AUTOCONFIG with Stateless)
IPv6 Address: fe80:2::2c0:f2ff:fe21:b8c4/64 Scope:Link
Status:UP/RUNNING(Enabled)/MTU 1500/LinkMTU is 1500
IPv6 Address: ::192.0.2.1/96 Scope:Global
Status:UP/RUNNING(Enabled)/MTU 1500/LinkMTU is 1500
>
```

Messages: *Active Configuration for IPv6: (AUTOCONFIG... xx seconds remaining)*

If a duplicate IPv6 address is discovered, a message displays at the bottom of the config listing; for example:

```
IPv6 Address: ::192.0.2.1/96 Scope:Global
[Duplicate] Status:UP/RUNNING(Enabled)/MTU 1500/LinkMTU is 1500
```

Command: **Set / Show IP DHCP Client Mode**

Syntax: **ip dhcp** [enable|disable]

Description: Set or show the DHCP client mode.

To enable or renew the S3280 DHCP client mode, type **ip dhcp enable** and press **Enter**.

To disable the S3280 DHCP client mode, type **ip dhcp disable** and press **Enter**.

To display the current S3280 DHCP client mode, type **ip dhcp** and press **Enter**.

The default is DHCP client mode disabled.

```

Example: >ip dhcp
DHCP Client      : Enabled

Active Configuration: (Static)
IP Address       : 192.168.1.110
IP Mask          : 255.255.255.0
IP Router        : 0.0.0.0
DNS Server       : 0.0.0.0
>ip dhcp disable
>ip dhcp
DHCP Client      : Disabled
>ip dhcp enable
>ip dhcp
DHCP Client      : Enabled

Active Configuration: (DHCP Processing...)
IP Address       : 0.0.0.0
IP Mask          : 0.0.0.0
IP Router        : 0.0.0.0
DNS Server       : 0.0.0.0
>
clear:/>

```

Note: you can not access S3280 by system name via DHCP/DNS.

Command: **IP Setup**

Syntax: **ip setup** [<ip_addr>] [<ip_mask>] [<ip_router>]

Description: Set or show the IPv4 setup, where:

<ip_addr> : IP address (a.b.c.d), default: Show IP address.

<ip_mask> : IP subnet mask (a.b.c.d), default: Show IP mask.

<ip_router>: IP router (a.b.c.d), default: Show IP router. The host part of the IP router can not be zero.

```

Example: >ip setup
IP Address       : 192.168.1.110
IP Mask          : 255.255.255.0
IP Router        : 192.168.1.1
DNS Server       : 0.0.0.0
VLAN ID         : 1
>

```

Messages: *The host part of the IP router is zero.* For example:

```

>ip setup 192.168.1.10 255.255.255.0 192.168.1.0
The host part of the IP router is zero
>

```

Command: IPv6 Setup**Syntax:** **ip>ipv6 setup** [<ipv6_addr>] [<ipv6_prefix>] [<ipv6_router>]**Description:** From the IP> menu path, set or show the IPv6 setup, where:

<ipv6_addr>: IPv6 address in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon to separate each field (:). For example, four hexadecimal digits with a colon (:) separates each field (e.g., 'fe80::215:c5ff:fe03:4dc7'). The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; however, it can only appear once. It can also be used to precede a valid IPv4 address (e.g., '::192.1.2.34').

<ipv6_prefix>: IPv6 subnet mask, default: Show IPv6 prefix. An IPv6 address prefix is a combination of an IPv6 prefix (address) and a prefix length. The prefix takes the form ipv6-prefix/prefix-length and represents a block of address space (or a network). The ipv6-prefix variable follows general IPv6 addressing rules (see [IETF RFC 2373](#)). The /prefix-length variable is a decimal value that indicates the number of contiguous, higher-order bits of the address that make up the network portion of the address. An example of a valid IPv6 prefix is 10FA:6604:8136:6502::/64. (Hexadecimal letters in IPv6 addresses are not case sensitive.)

<ipv6_router>: IPv6 router. The default is Show IPv6 router. An IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon to separate each field (:). In the example, 'fe80::215:c5ff:fe03:4dc7', the symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also be used to precede a valid IPv4 address (e.g., '::192.1.2.34').

Example 1: Type **ip setup** and press **Enter** to set or show the current S3280 IPv6 setup parameters.**>ip ipv6 setup**

```
IPv6 AUTOCONFIG mode      : Enabled (Fallback in 300 seconds)
IPv6 Link-Local Address: fe80::2c0:f2ff:fe21:b8c4
IPv6 Address              : ::192.168.0.1
IPv6 Prefix               : 96
IPv6 Router               : ::
```

> Example 2: **IP>ipv6 setup ::192.168.1.30 2 fe80::215:c5ff:fe03:4dc7****IP>ipv6 setup**

```
IPv6 AUTOCONFIG mode      : Enabled (Fallback in 300 seconds)
IPv6 Link-Local Address: fe80::2c0:f2ff:fe00:1
IPv6 Address              : ::192.168.1.30
IPv6 Prefix               : 2
IPv6 Router               : fe80::215:c5ff:fe03:4dc7
IP>
```

Command: IPv4 Ping

Syntax: **ip ping** <ip_addr_string> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)]

Description: From the IP> menu path, Ping an IPv4 address (ICMP echo), where:

<ip_addr_string>: IP host address (a.b.c.d) or a host name string.

length : PING Length keyword.

<ping_length> : Ping ICMP data length (2-1452; Default is 56), excluding MAC, IP and ICMP headers.

count : PING Count keyword.

<ping_count> : Transmit ECHO_REQUEST packet count (1-60; Default is 5).

interval : PING Interval keyword.

<ping_interval> : Ping interval (0-30; Default is 0).

Example:

```
>ip ping 192.168.1.30
PING server 192.168.1.30, 56 bytes of data.
64 bytes from 192.168.1.30: icmp_seq=0, time=0ms
64 bytes from 192.168.1.30: icmp_seq=1, time=0ms
64 bytes from 192.168.1.30: icmp_seq=2, time=0ms
64 bytes from 192.168.1.30: icmp_seq=3, time=0ms
64 bytes from 192.168.1.30: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
>
```

Command: IPv6 Ping

Syntax: **IPv6 Ping6** <ipv6_addr> [<ping_length>] [<ping_count>]

Description: Ping IPv6 address (ICMPv6 echo), where:

<ipv6_addr> : IPv6 host address.

IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address.

For example, ':::192.1.2.34'.

length : PING Length keyword

<ping_length> : Ping ICMP data length (2-1452; Default is 56), excluding MAC, IP and ICMP headers

count : PING Count keyword

<ping_count> : Transmit ECHO_REQUEST packet count (1-60; Default is 5)

interval : PING Interval keyword

<ping_interval>: Ping interval (0-30; Default is 0)

Example:

```
IP>ipv6 ping fe80::215:c5ff:fe03:4dc7
PING6 server fe80::215:c5ff:fe03:4dc7
recvfrom: Operation timed out
recvfrom: Operation timed out
recvfrom: Operation timed out
recvfrom: Operation timed out
recvfrom: Operation timed out
Sent 5 packets, received 0 OK, 0 bad
IP>
```

Command: **IP IPv6 AUTOCONFIG**
Syntax: **ip ipv6 autoconfig** [enable|disable]
Description: Set or show the IPv6 AUTOCONFIG mode, where:
enable : Enable the IPv6 Autoconfiguration mode.
disable: Disable IPv6 Autoconfiguration mode.
Fallback Timer: (36-3600) Seconds; Default is 300.

Example:

```
>ip ipv6 autoconfig

IPv6 AUTOCONFIG mode      : Enabled (Fallback in 300 seconds)
IPv6 Link-Local Address:  fe80::2c0:f2ff:fe21:b8c4
IPv6 Address              :  ::192.0.2.1
IPv6 Prefix                :  96
IPv6 Router               :  ::
>
```

IPv6 Parameter Descriptions:

IPv6 AUTOCONFIG mode - if IPv6 auto-configuration is enabled and it fails, the configured IPv6 address is zero. The router may delay responding to a router solicitation for a few seconds, the total time needed to complete auto-configuration can be significantly longer.

IPv6 Link-Local Address of this S3280. One of IPv6 addresses for local link usage. In IPv6, an address having link-only scope that can be used to reach neighboring nodes attached to the same link. All interfaces have a link-local unicast address. An IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon (:) separating each field (e.g., 'fe80::215:c5ff:fe03:4dc7'). The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; however, it can only appear once. The symbol '::' can also represent a valid IPv4 address (e.g., '::192.1.2.34').

IPv6 Address -the IPv4 address preceded by the symbol '::' (e.g., ::192.0.2.1).

IPv6 Prefix - the IPv6 Prefix of this S320. The valid range is 1 to 128.

IPv6 Router - the IPv6 gateway address of this S3280. An IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon (:) separating each field (e.g., 'fe80::215:c5ff:fe03:4dc7'). The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; however, it can only appear once. The symbol '::' can also represent a valid IPv4 address (e.g., '::192.1.2.34').

Command: IP DNS

Syntax: ip dns [<ip_addr>]

Description: Set or show the DNS server IP address, where:
<ip_addr>: IP address (a.b.c.d). The default is 'Show' the current DNS server's IP address.

Example:

```
>ip dns
DNS Server      : 0.0.0.0
>ip dns 192.168.1.30
>ip dns
DNS Server      : 192.168.1.30
>
clear:/>
```

Note: you can not access S3280 by system name via DHCP/DNS.

Command: IP DNS_Proxy

Syntax: ip dns_proxy [enable|disable]

Description: Set or show the IP DNS Proxy mode. This command enables or disables the DNS Proxy server function, or displays the current DNS Proxy server configuration.
When DNS Proxy is enabled, the S3280 will relay DNS requests to the currently configured DNS server on the S3280, and reply as a DNS resolver to the client device on the network.
Note that setting this function does not provide the full set of IP, BootP, VLAN, DNS server, and Management VLAN / member ports configuration. Note that the underscore (_) character is required. The **ip dns_proxy** command parameters are:
enable: Enable DNS Proxy.
disable: Disable DNS Proxy.

Example:

```
>ip dns_proxy
DNS Proxy       : Disabled
>ip dns_proxy enable
>ip dns_proxy
DNS Proxy       : Enabled
>
```

Command: IP Mvlan

Syntax: ip mvlan [<vid>]

Description: Set or show the S3280 Management VLAN. To set the Management VLAN ID, provide the managed VLAN ID in the range of 1-4094. A VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs. The valid range is 1 to 4094 for this Management VLAN ID. This Management VLAN provides a secure channel for all management traffic to/from the device. **Note:** Be sure to set the Management VLAN configuration before you set the VLAN configuration. The **ip mvlan** command parameters are:
<vid>: VLAN ID (1-4094).

Example:

```
>ip mvlan
IP Address      : 192.168.1.110
IP Mask         : 255.255.255.0
IP Router       : 0.0.0.0
DNS Server      : 192.168.1.30
VLAN ID        : 1
>ip mvlan 2
>ip mvlan
IP Address      : 192.168.1.110
IP Mask         : 255.255.255.0
IP Router       : 192.168.1.1
DNS Server      : 192.168.1.30
VLAN ID        : 2
```


>

Command: IP NTP Configuration**Syntax:** ip ntp configuration

Description: Show the current NTP configuration. Network Time Protocol (NTP) is a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer. The S3280 uses NTP for real time clock synchronization with the network time server. The NTP is compliant with IETF RFC 5905. The S3280 takes care of day light saving options where used. The management interfaces provide options to configure NTP and report the network time synchronized. The S3280 time obtained is used for all S3280 services that need a timestamp.

Example: >ip ntp config

```

IP NTP Configuration:
=====

NTP Mode : Disabled
Idx   Server IP host address (a.b.c.d) or a host name string
----  -
1
2
3
4
5
>

```

Command: IP NTP Mode**Syntax:** ip ntp mode [enable|disable]**Description:** Set or show the NTP mode, where:**enable** : Enable NTP mode.**disable** : Disable NTP mode.

(The default is 'Show' NTP mode.)

Type **ip ntp mode** and press **Enter** to display the current NTP mode (Enabled or Disabled).Type **ip ntp mode enable** and press **Enter** to enable NTP mode. The default is Disabled.

When NTP mode operation is enabled, the agent forwards NTP messages between the clients and the server when they are not on the same subnet domain.

Example: >ip ntp mode

```

NTP Mode : Disabled
>ip ntp mode enable
>ip ntp mode
NTP Mode : Enabled
>

```

Command: Add IPv4 NTP Server**Syntax:** `ip ntp server add <server_index> <ip_addr_string>`**Description:** Adds a new IPv4 NTP Server entry to the S3280 configuration. Up to five IPv4 NTP Servers can be configured.Type `ip ntp server add <server index x> <ip addr string y>` and press **Enter** to add an NTP Server, where:`<server_index>` = the number of this NTP Server (i.e., 1 = the first IPv4 NTP server, 2 = the second, etc.).`<ip_addr_string>` = the IP address of this IP v4 NTP Server (e.g., 192.168.1.30).**Example:**

```

>ip ntp server add 1 192.168.1.30
>ip ntp config

IP NTP Configuration:
=====

NTP Mode : Enabled
Idx   Server IP host address (a.b.c.d) or a host name string
---   -
1     192.168.1.30
2
3
4
5
>

```

Command: Add IPv6 NTP Server**Syntax:** `ip ntp server ipv6 add <server_index> <server_ipv6>`**Description:** Adds a new IPv6 NTP Server to the S3280 configuration. Up to 5 IPv6 NTP Servers can be configured.Type `ip ntp server ipv6 add <server index x> <ip addr string y>` and press **Enter** to add an NTP Server, where:`<server_index>`: the number of this IPv6 NTP Server (i.e., 1 = the first IPv6 NTP server, 2 = the second ipv6 NTP server, etc.).`<server_ipv6>`: the IP address of this IPv6 NTP Server (e.g., 192.168.1.30).

An IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon to separate each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'.

The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used with a following legal IPv4 address (e.g., '::192.1.2.34').

Example:

```

>ip ntp server ipv6 add 1 fe80::215:c5ff:fe03:4dc7
>

```

Command: IP NTP Server Delete**Syntax:** `ip ntp server delete <server_index>`**Description:** Deletes an existing IPv4 or IPv6 NTP Server from the S3280 configuration.Type `ip ntp server delete <server_index x>`, where:`<server_index>`: the number of this NTP Server (i.e., 1 = the first NTP server, 2 = the second, etc.).**Example:**

```

IP>ntp server ipv6 add 2 fe80::215:c5ff:fe03:4dc7
IP>ntp server delete 2
IP>

```

Messages: *Doesn't allowed to delete empty server*

Port Commands

These S3280 Port group commands provide Port management, statistics, SFP and related port configuration.

>port ?

Available Commands:

Port Configuration [<port_list>] [up|down]

Port Mode [<port_list>] [auto|10hdx|10fdx|100hdx|100fdx|1000fdx|2500fdx|sfp_auto_ams]

Port Flow Control [<port_list>] [enable|disable]

Port State [<port_list>] [enable|disable]

Port MaxFrame [<port_list>] [<max_frame>]

Port Power [<port_list>] [enable|disable|actiphy|dynamic]

Port Excessive [<port_list>] [discard|restart]

Port Statistics [<port_list>] [<command>] [up|down]

Port VeriPHY [<port_list>]

Port SFP [<port_list>]

Port DMI Configuration [<port_list>] [<dmi_rx_pwr_int_thr>]

Port DMI Statistics [<port_list>]

Port Description [<port_list>] [<name>]

>

Command: **Port Configuration**

Syntax: **port configuration** [<port_list>] [up|down]

Description: Displays the current port configuration. Type **port config** and press **Enter** to display the full set of current port parameters, where:

<port_list>: Port list or 'All'. The default is 'All' ports.

up : Show ports which are up.

down : Show ports which are down.

Example:

```
>port config
```

```
Port Configuration:
=====
```

Port	State	Mode	Flow Control	MaxFrame	Power	Excessive	Link
1	Enabled	Auto	Disabled	9600	Disabled	Discard	100fdx
2	Enabled	Auto	Disabled	9600	Disabled	Discard	Down
3	Enabled	Auto	Disabled	9600	Disabled	Discard	Down
4	Enabled	Auto	Disabled	9600	Disabled	Discard	Down
5	Enabled	Auto	Disabled	9600	Disabled	Discard	Down
6	Enabled	Auto	Disabled	9600	Disabled	Discard	Down
7	Enabled	Auto	Disabled	9600	Disabled	Discard	Down
8	Enabled	Auto	Disabled	9600	Disabled	Discard	100fdx
9	Enabled	Auto	Disabled	1522	Disabled	Discard	Down

```
>port config up
```

```
Port Configuration:
=====
```

Port	State	Mode	Flow Control	MaxFrame	Power	Excessive	Link
1	Enabled	Auto	Disabled	9600	Disabled	Discard	100fdx
8	Enabled	Auto	Disabled	9600	Disabled	Discard	100fdx

```
>
```

Command: Port Mode**Syntax:** port mode [<port_list>] [auto|10hdx|10fdx|100hdx|100fdx|1000fdx|2500fdx]**Description:** Set or show the port speed and duplex mode. Type **port mode** and press **Enter** to display the port / mode / list table, where:

<port_list>: Port list or 'All'. The default is 'All ports'.

auto : Auto negotiation of speed and duplex.**10hdx** : 10 Mbps, half duplex.**10fdx** : 10 Mbps, full duplex.**100hdx** : 100 Mbps, half duplex.**100fdx** : 100 Mbps, full duplex.**1000fdx** : 1 Gbps, full duplex.**2500fdx** : proprietary 2.5 Gbps, full duplex mode. Ports 7 and 8 only.**sfp_auto_ams**: Auto detection of SFP.

(The default is 'Show configured and current mode'.)

Example:

```

>port mode
Port  Mode          Link
----  -
1      Auto             100fdx
2      Auto             Down
3      Auto             Down
4      Auto             Down
5      Auto             Down
6      Auto             Down
7      Auto             Down
8      Auto             Down
9      Auto             Down
>port mode 1 2500fdx
Port 1 does not support this mode
>port mode 6 2500fdx
Port 6 does not support this mode
>port mode 7 2500fdx
>port mode 8 2500fdx
>port mode 9 2500fdx
Port 9 does not support this mode
>port mode 10 2500fdx
Invalid parameter: 10

Syntax:
Port Mode [<port_list>]
[auto|10hdx|10fdx|100hdx|100fdx|1000fdx|2500fdx|sfp_auto_ams]
>port mode

Port  Mode          Link
----  -
1      Auto             100fdx
2      Auto             Down
3      Auto             Down
4      Auto             Down
5      Auto             Down
6      Auto             Down
7      2.5Gfdx         Down
8      2.5Gfdx         Down
9      Auto             Down
>

```

Messages: An “*Invalid parameter*” message displays if the entered port number does not support the selected mode (e.g., “*Port 1 does not support this mode*” or “*Port 12 does not support this fiber mode*”).

Note: When a twisted-pair port is set to Auto-Negotiation, the end node should also be set to Auto-Negotiation to prevent a duplex mode mismatch. A port using Auto-Negotiation defaults to half-duplex if it detects that the end node is not using Auto-Negotiation. This can result in a mismatch if the end node is operating at a fixed duplex mode of full-duplex. To avoid this problem when connecting an end node with a fixed duplex mode of full-duplex to a switch port, disable Auto-Negotiation on the port and set the port’s speed and duplex mode manually.

Command: Port Flow Control**Syntax:** port flow control [<port_list>] [enable|disable]

Description: Set or show the port flow control mode, where:
 <port_list>: Port list or 'all', default: All ports.
enable : Enable flow control for this port.
disable : Disable flow control for this port.
 (default: Show flow control mode)

Type **port flow control ?** and press **Enter** to display the port mode command's description and syntax.

Type **port flow control** and press **Enter** to display the current Port / FC / RX/TX Pause configuration settings.

Example: >port flow control 1,2,3 enable
 >port flow control

Port	Flow Control	Rx Pause	Tx Pause
1	Enabled	Disabled	Disabled
2	Enabled	Disabled	Disabled
3	Enabled	Disabled	Disabled
4	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled
9	Disabled	Disabled	Disabled

Command: Port State**Syntax:** port state [<port_list>] [enable|disable]**Description:** Set or show the current S3280 port administrative state.

Type **port state** and press **Enter** to display the current S3280 ports' admin states (Enabled or Disabled). By default all ports admin states are displayed.

Type **port state 1,2** and press **Enter** to display the current administrative states of S3280 ports 1 and 2.

Example: >port state 3,4,5 disable
 >port state

Port	State
1	Enabled
2	Enabled
3	Disabled
4	Disabled
5	Disabled
6	Enabled
7	Enabled
8	Enabled
9	Enabled

Command: **Port MaxFrame**

Syntax: **port maxframe** [<port_list>] [<max_frame>]

Description: Set or show the port maximum frame size, where:

<port_list>: Port list or 'All'. The default is 'All' ports.

<max_frame>: Port maximum frame size (1518-9600). The default is 'Show maximum frame size'. The default for Ports 1-8 is 9600. The default for Port 9 is 1522.

Example:

```
>port maxframe
Port  MaxFrame
----  -
1      9600
2      9600
3      9600
4      9600
5      9600
6      9600
7      9600
8      9600
9      1522
>port maxframe 4,5,6 1522
port maxframe
Port  MaxFrame
----  -
1      9600
2      9600
3      9600
4      1522
5      1522
6      1522
7      9600
8      9600
9      1522
>
```

An “*Invalid parameter*” message displays if you try to enter a value outside of the valid range of 1518-9600 packets (e.g., *Invalid parameter: 9999* displays).

Command: Port Power**Syntax:** port power [<port_list>] [enable|disable|actiphy|dynamic]**Description:** Set or show the port PHY power mode, where:

<port_list>: Port list or 'All'. The default is All ports.

enable : Enable all power control. Supported on S3280 Ports 1-4 (copper ports).**Disable** : Disable all power control. Supported on all S3280 Ports.**Actiphy** : Enable the ActiPHY power control. ActiPHY™ is an automatic power savings mode when a specific port is in link down or standby operation. Supported on S3280 Ports 1-4.**Dynamic** : Enable Dynamic power control (controls transmit power and reduces power during idle periods). Supported on S3280 Ports 1-4.**Example:**

```

>port power
Port  Power
----  -
1      Disabled
2      Disabled
3      Disabled
4      Disabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
9      Disabled
>port power enable
Port 5 does not support this mode
Port 6 does not support this mode
Port 7 does not support this mode
Port 8 does not support this mode
>port power
Port  Power
----  -
1      Enabled
2      Enabled
3      Enabled
4      Enabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
9      Enabled
>port power 5,6 actiphy
Port 5 does not support this mode
Port 6 does not support this mode
>port power 5,6 dynamic
Port 5 does not support this mode
Port 6 does not support this mode
>port power 1,3 actiphy
>port power
Port  Power
----  -
1      ActiPHY
2      Enabled
3      ActiPHY
4      Enabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
9      Enabled
>port power 2 dynamic
>port power

```



```

Port   Power
-----
1      ActiPHY
2      Dynamic
3      ActiPHY
4      Enabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
9      Enabled
>

```

Note that not all S3280 ports support all of the command options. If not supported, a message like “*Port 8 does not support this mode*” displays. Note that in the ‘show’ version of this command, Port 9 displays in the table as ‘Disabled’; however, Port 9 can not be assigned a value using the ‘set’ version of this command. Changing the mode may display the message “*Local Area Network Connection x. A network cable is unplugged*”. Actiphy® is a registered trademark owned by Vitesse Semiconductor Corporation.

Command: **Port Excessive Collision Mode**

Syntax: **port excessive** [<port_list>] [discard|restart]

Description: Set or show the port excessive collision mode, where:

<port_list>: Port list or 'all', default: All ports.

discard : Discard frame after 16 collisions.

restart : Restart backoff algorithm after 16 collisions. **Note:** Ports 5 - 8 do not support the **port excessive restart** mode.

(default: Show mode)

Example:

```

>port excessive

Port   Excessive
-----
1      Discard
2      Discard
3      Discard
4      Discard
5      Discard
6      Discard
7      Discard
8      Discard
9      Discard
>port excessive 2,3,4 restart
>port excessive

Port   Excessive
-----
1      Discard
2      Restart
3      Restart
4      Restart
5      Discard
6      Discard
7      Discard
8      Discard
9      Discard
>

```

Command: Port Statistics**Syntax:** **port statistics** [<port_list>] [<command>] [up|down]**Description:** Show the current port statistics, where:

<port_list>: Port list or 'All'. The default is 'All' ports (can be a long listing).

<command> : The command parameter takes the following values:

clear : Clear port statistics.**packets** : Show packet statistics.**bytes** : Show byte statistics.**errors** : Show error statistics.**discards** : Show discard statistics.**filtered** : Show filtered statistics.**0..7** : Show priority statistics.

(The default is 'Show all port statistics'.)

up : Show ports, which are up.**down** : Show ports, which are down.

(default: Show all ports)

Example 1:

```

>port statistics 1,2 packets
Port  Rx Packets          Tx Packets
-----
1      0                    435
2      0                    435
>port statistics 1,2 errors
Port  Rx Errors           Tx Errors
-----
1      0                    0
2      0                    0
>port statistics 1,2 discards
Port  Rx Discards         Tx Discards
-----
1      0                    0
2      0                    0
>port statistics filtered
Port  Rx Filtered
-----
1      10
2      0
3      0
4      0
5      8
6      0
7      0
8      0
9      0
>

```

A sample **port statistics** command is shown below (for port 1 down):

```

>port statistics 1 down
>port statistics 1 up
Port 1 Statistics:

Rx Packets:                3972    Tx Packets:                4871
Rx Octets:                 1052597  Tx Octets:                 1265434
Rx Unicast:                3791    Tx Unicast:                2649
Rx Multicast:              2        Tx Multicast:              2210
Rx Broadcast:              179    Tx Broadcast:              12
Rx Pause:                  0        Tx Pause:                  0

Rx 64:                    2031    Tx 64:                    1445
Rx 65-127:                185    Tx 65-127:                971
Rx 128-255:               24        Tx 128-255:              1561
Rx 256-511:               804    Tx 256-511:               388
Rx 512-1023:              926    Tx 512-1023:              112
Rx 1024-1526:             2        Tx 1024-1526:            394
Rx 1527- :                0        Tx 1527- :                0

Rx 0:                     3972    Tx 0:                     0
Rx 1:                     0        Tx 1:                     0
Rx 2:                     0        Tx 2:                     0
Rx 3:                     0        Tx 3:                     0
Rx 4:                     0        Tx 4:                     0
Rx 5:                     0        Tx 5:                     0
Rx 6:                     0        Tx 6:                     0
Rx 7:                     0        Tx 7:                     4871

Rx Drops:                  0        Tx Drops:                  0
Rx CRC/Alignment:         0        Tx Late/Exc. Coll.:       0
Rx Undersize:              0
Rx Oversize:               0
Rx Fragments:              0
Rx Jabbers:                0
Rx Filtered:               0
>

```

Command: Port VeriPHY

Syntax: port veriphy [<port_list>]

Description: Runs the cable diagnostic test and displays the resulting cable pair test results, where:

<port_list>: Port list or 'All'. The default is 'All' ports

After the message "Starting VeriPHY, please wait" clears, the test data displays.

OK - the pair is operational.

Open - the pair has an open in the circuit.

Short - the pair has a short in the circuit.

Length - the distance to the fault (far end device) in meters.

Example:

```
>port veriphy 1
Starting VeriPHY, please wait
Port   Pair A   Length   Pair B   Length   Pair C   Length   Pair D   Length
-----
1      Open     0        Open     0        Open     0        Open     0
>port veriphy 1,2,3
Starting VeriPHY, please wait
>port ver
Starting VeriPHY, please wait
Port   Pair A   Length   Pair B   Length   Pair C   Length   Pair D   Length
-----
1      Open     0        Open     0        Open     0        Open     0
2      Open     0        Open     0        Open     0        Open     0
3      OK       3        OK       3        Short    0        Short    0
4      Open     0        Open     0        Open     0        Open     0
>
```

When all of the information has displayed, the initial command prompt information displays.

The VERIPHY trademark was assigned a serial number by the USPTO June 11, 2002 (Type Of Mark: Service Mark). The current federal status of this trademark filing is Cancelled - Section 8.

Command: Port SFP

Syntax: Port SFP [<port_list>]

Description: Displays the detected SFP type, where:
 <port_list>: Port list or 'All'. The default is 'All' ports.

Example:

```
>port sfp
```

Port	SFP type	Vendor name	Vendor PN	Rev	MAC_IF
1	None				SGMII
2	None				SGMII
3	None				SGMII
4	None				SGMII
5	10G	Transition	TN-10GSFP-SR	0001	SERDES
6	10G	AVAGO	AFBR-703SDZ-NA1	G2.3	SERDES
7	1000BASE_SX	Transition	TN-SFP-SXD	0000	SERDES
8	None				SERDES
9	None				SGMII

```
>
```

The **MAC_IF** column parameters include:

SERDES (Serializer/Deserializer) is a pair of functional blocks used in S3280 communications to ompensate for limited input/output.

SGMII (Serial Gigabit Media Independent Interface) is a standard interface used to connect an Ethernet MAC-block to a PHY. SGMII is used for GbE and can also carry 10/100 MBit Ethernet.

Command: Port DMI Configuration**Syntax:** `port dmi config [<port_list>] [<dmi_rx_pwr_int_thr>]`**Description:** This command displays the DMI (Diagnostic Monitoring Interface) port configuration in terms of Interface Characteristics, Diagnostic Monitoring, and Supported Media Length.

The S3280 supports connectors with DMI (SFF-8472) capability. All DMI events will trigger notification. Intrusion detection based on Rx Power level is available for triggering any drop in the Rx power. The DMI function displays S3280 diagnostic / maintenance information such as fiber interface characteristics, diagnostic monitoring parameters, and supported fiber media lengths. The S3280 supports connectors with DMI (SFF-8472) capability. All DMI events will trigger notification. Intrusion detection, based on Rx Power level, is available for triggering any drop in the Rx power. Note that S3280 DMI support requires an SFP that supports DMI.

Note that DMI statistics are cleared whenever an SFP is removed.

Use the **port dmi config** command to set or show the port DMI: Receive Power Intrusion Threshold, where:

<port_list> : Port list or 'all', default: All ports.

<dmi_rx_pwr_int_thr>: Port DMI receive power intrusion threshold (0-65535). This is a configurable level for Rx Power on the Fiber port. If the DMI read value falls below the set value, an intrusion is detected, and a trap is generated. The default is 0 uW (microWatts). The valid range is 0 – 65,535 uW (microWatts).

This command defines the lowAlarm threshold for RxPowerAlarm. If a non-zero value (in microwatts) is specified, the S3280 will stop passing traffic when the receive power drops below the new threshold. This feature is sometimes referred to as Intrusion Detection, since tapping into a fiber to intercept traffic leads to a reduction in receive power.

Sets the Diagnostic Monitoring Interface (DMI) receive preset power level for a fiber port.

Example:

```
>port dmi config

Port  RxPwrIntThr
----  -
1     n/a
2     n/a
3     n/a
4     n/a
5     0
6     0
7     0
8     0
9     n/a
>
```

Command: **Port DMI Statistics**
Syntax: **port dmi statistics** [<port_list>]
Description: Show DMI port statistics, where:
 <port_list>: Port list or 'All'. The default is 'All' ports.

```

Example: >port dmi stat 6
Port 6 DMI Statistics:
-----
DMI ID:                Unknown or unspecified
>port dmi stat 5
Port 5 DMI Statistics:
-----
DMI ID:                SFP transceiver
Connector Type:       LC
Nominal Bit Rate:     1300 Mbps
Wavelength:           850 nm
RX Power uW:          252 uW
RX Power dBm:         -5.98 dBm
RX Power Alarm:       Normal
RX Power Int Thr uW:  0 uW
Temperature C:        44 C
Temperature F:        111 F
Temperature Alarm:    Normal
TX Bias:              4832 uA
TX Bias Alarm:        Normal
TX Power uW:          253 uW
TX Power dBm:         -5.96 dBm
TX Power Alarm:       Normal
Length 9/125:         0 meters
Length 50/125:        500 meters
Length 62.5/125:     300 meters
Length Copper:        0 meters
Vendor Name:          Transition
Vendor OUI:           00-C0-F2
Vendor Part Number:   TN-SFP-SXD
Vendor Part Rev:      000
Vendor Serial No:     8672002
>

```

Note: The DMI commands can only be entered for a fiber port that supports DMI. Not all S3280 ports support DMI. Transition Networks SFPs that support DMI have a “D” at the end of the model number. If you enter a DMI command on a S3280 port that does not support DMI, the message “*The DMI feature is not supported on current port.*” displays.

Note that DMI statistics are cleared whenever an SFP is removed. When an SFP is removed, the command displays *DMI ID: Unknown or unspecified*. When the SFP is replaced, the DMI statistics then re-display.

The DMI statistics parameters are explained below.

DMI ID: Specifies the physical device from SFF-8472 Rev 9.5 Standard. The valid values are:

- Unknown or unspecified** (00h).
- GBIC** (Gigabyte Interface Converter) (01h).
- Module/connector soldered to motherboard** (02h).
- SFP transceiver** (03h).
- Reserved** (04-7Fh).
- Vendor specific** (80-FFh).

Connector Type: The external optical or electrical cable connector provided as the interface. Valid values are:

MT-RJ: Media Termination - Recommended Jack for Duplex multimode connections.

LC: Lucent Connector or Local Connector for High-density connections, SFP transceivers.

SC: Subscriber Connector for Datacomm and Telecomm.

ST: BFOC Straight Tip / Bayonet Fiber Optic Connector for Multimode - rarely Singlemode (APC not possible).

VF-45: Snap connector for Datacom uses.

Unknown or unspecified: interface connector information not provided.

Nominal Bit Rate (Mbps): The measured Bitrate in units of 100Mbps (e.g., **1300**, or 1.3 Gbps).

Wavelength (nm): The Nominal Fiber Interface transmitter output wavelength at room temperature. The unit of measure is nanometers (e.g., **850** nm measured wavelength).

Rx (μ W): Receive power on local fiber measured in microwatts (e.g., **11** μ W) (measured power).

Rx Power (dBm): Receive power on local fiber measured in dBm (decibels relative to one milliwatt) which defines signal strength (e.g., **-19.586** dBm).

Rx Power Alarm: Alarm status for receive power on local fiber (measured signal strength). The dmi_alarm_types are **Normal, Not Supported, Low Warn, High Warn, No, Low Alarm, and High Alarm.**

Rx Power Intrusion Threshold: A preset level for Rx Power on the Fiber port. If the DMI read value falls below the preset value, an intrusion is detected, and a trap is generated. The default is **0** μ W. The valid range is **0 – 65,535** uW.

Temperature ($^{\circ}$ C): Temperature of fiber transceiver in tenths of degrees C (Celsius) (e.g., **40.1** $^{\circ}$ C measured temp.).

Temperature ($^{\circ}$ F): Temperature of fiber transceiver in tenths of degrees F (Fahrenheit) (e.g., **104.2** $^{\circ}$ F measured temp.).

Temperature Alarm: Alarm status for temperature of fiber transceiver. An event is sent when there is a warning or alarm on DMI temperature. The dmi_alarm_types are **Normal, Not Supported, Low Warn, High Warn, No, Low Alarm, and High Alarm.**

Tx Bias: Transmit bias current on local fiber interface, in μ A (microamperes) (e.g., **14768** uA (microamps) measured current).

Tx Bias Alarm: Alarm status for transmit bias current on local fiber interface. The alarm types are **Normal, Not Supported, Low Warn, High Warn, No, Low Alarm, and High Alarm.**

Tx Power (μ W): Transmit power on local fiber measured in microwatts (e.g., **240** μ W (microwatts) measured power).

Tx Power (dBm): Transmit power on local fiber measured in dBm (decibels relative to one milliwatt) which defines signal strength (e.g., **-6.126** dBm measured power).

Tx Power Alarm: Alarm status for transmit power on local fiber. The dmi_alarm_types are **Normal, Not Supported, Low Warn, High Warn, No, Low Alarm, and High Alarm.**

Length 9/125: Specifies the link length that is supported by the transceiver while operating in single mode (SM) fiber. The unit of measure is meters (m). Displays **N/A** if the media is not applicable.

Length 50/125: Specifies the link length that is supported by the transceiver while operating in 50 micron Multimode (MM) fiber. The value is in meters (m) (e.g., **500** meters as the supported media length).

Length 62.5/125: Specifies the link length that is supported by the transceiver while operating in 62.5 micron Multimode (MM) fiber. The value is in meters (m) (e.g., **300** meters as the supported media length).

Length Copper: Specifies the link length that is supported by the transceiver while operating in copper cable. The value is in meters (m). Displays **N/A** to indicate the media is not applicable.

Vendor Name: The name of the SFP manufacturer (e.g., ABC Corp.).

Vendor OUI: The SFP's Organizationally Unique Identifier (e.g., 00-C0-F2)

Vendor Part Number: The SFP manufacturer's assigned part number (e.g., TN-SFP-SXD).

Vendor Part Rev: The SFP manufacturer's assigned part version number or revision (e.g., 000).

Vendor Serial No: The SFP manufacturer's assigned serial number (e.g., 8672002).

Note that these DMI statistics are cleared whenever an SFP is removed.

Command: Port Description**Syntax:** port description [<port_list>] [<name>]**Description:** Set or show the port's descriptive name, where:

<port_list>: Port list or 'All'. The default is 'All ports'.

<name> : Port Description name of up to 31 characters. Use "" (open and closing quote characters) to reset the description. The description "n/s" displays to indicate that no string name has been assigned.

Example:

```

>port descr

Port  Description
----  -
1     n/s
2     n/s
3     n/s
4     n/s
5     n/s
6     n/s
7     n/s
8     n/s
9     n/s

>port descr 1 cuport1
>port descr 2 cuport2
>port descr 5 fbrport1
>port descr 6 fbrport2
>port descr 9 MGMT_port
>port descr

Port  Description
----  -
1     cuport1
2     cuport2
3     n/s
4     n/s
5     fbrport1
6     fbrport2
7     n/s
8     n/s
9     MGMT_port

>port descr 9 ""
>port descr

Port  Description
----  -
1     cuport1
2     cuport2
3     n/s
4     n/s
5     fbrport1
6     fbrport2
7     n/s
8     n/s
9     n/s

```

MAC Commands

Frames switching is based on the DMAC address contained in the frame. The S3280 builds a table that maps MAC addresses to S3280 ports for knowing which ports the frames should go to (based on the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if a fixed mapping between the DMAC address and S3280 ports is desired.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the S3280 to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frames with the corresponding SMAC address have been seen after a configurable age time.

These S3280 commands provide MAC address table configuration functions.

>**mac ?**

Available Commands:

```

MAC Configuration [<port_list>]
MAC Add <mac_addr> <port_list> [<vid>]
MAC Delete <mac_addr> [<vid>]
MAC Lookup <mac_addr> [<vid>]
MAC Agetime [<age_time>]
MAC Learning [<port_list>] [auto|disable|secure]
MAC Dump [<mac_max>] [<mac_addr>] [<vid>]
MAC Statistics [<port_list>]
MAC Flush
>

```

The S3280 MAC address table configuration commands are explained below.

Command: **MAC Configuration**

Syntax: **mac configuration** [<port_list>]

Description: Displays the current S3280 MAC address table configuration for a specified port or for all ports.

Example: >**mac config**

```

MAC Configuration:
=====

MAC Address : 00-c0-f2-21-b8-c4
MAC Age Time: 300

Port  Learning
----  -
1     Auto
2     Auto
3     Auto
4     Auto
5     Auto
6     Auto
7     Auto
8     Auto
>

```

Command: MAC Add**Syntax:** **mac add** <mac_addr> <port_list> [<vid>]**Description:** Adds (creates) a new MAC address entry to the S3280 MAC Addresses table, where:
<mac_addr> : MAC address (xx-xx-xx-xx-xx-xx)
<port_list>: Port list or 'all' or 'none'.
<vid> : VLAN ID (1-4094), default: 1.**Example:**
>**mac add 11-11-11-11-11-11 all 1**
>**Note:** Use the **mac config** command to display the current MAC addresses.**Command: MAC Delete****Syntax:** **mac delete** <mac_addr> [<vid>]**Description:** Deletes the specified (existing) MAC address from the MAC Addresses table, where:
<mac_addr>: MAC address (xx-xx-xx-xx-xx-xx).
<vid> : VLAN ID (1-4094), default: 1.**Example:**
>**mac delete 11-11-11-11-11-11 1**
>**mac delete 11-11-11-11-11-11 1**
mac table del operation failed
>If the specified MAC address has already been deleted or has not yet been created, the message “*mac table del operation failed*” displays.**Command: MAC Lookup****Syntax:** **mac lookup** <mac_addr> [<vid>]**Description:** Displays a MAC address entry, where:
<mac_addr>: MAC address (xx-xx-xx-xx-xx-xx).
<vid> : VLAN ID (1-4094), default: 1.**Example:**
>**mac lookup 00-c0-f2-ff-ff-10 1**
Type VID MAC Address Ports
----- - -----
Static 1 00-c0-f2-ff-ff-10 None,CPU
>If the specified MAC address or VID has already been deleted or has not yet been created, the message “*MAC address not found*” displays.

Command: **MAC Agetime**

Syntax: **mac agetime** [<age_time>]

Description: Set or show the MAC Address table Aging Configuration. By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging. Configure the aging time by entering a value here in seconds. The valid range is 10 to 1000000 seconds (11.57 days). A value of 0 disables the MAC aging time. Note that when aging is disabled, the FDB size can grow to a maximum of 8000 entries. After the maximum limit of the MAC limit is reached, the new MAC entries are added and the older dynamic MAC entries are purged from the database. The parameters are:
<age_time>: MAC address age time (0, 10-1,000,000).

Example:

```
>mac agetime
MAC Age Time: 300
>mac agetime 600
>mac agetime
MAC Age Time: 600
>
```

Command: **MAC Learning**

Syntax: **mac learning** [<port_list>] [auto|disable|secure]

Description: Sets (defines) or shows (displays) the current MAC Table Learning Mode. If the learning mode for a given port is grayed out, another module is in control of the mode, so that it cannot be changed by a user. An example of such a module is the MAC-Based Authentication under 802.1X. Each port can do learning based on the following settings:
auto - Learning is done automatically as soon as a frame with unknown SMAC is received.
disable - No learning is done.
secure - Only static MAC entries are learned, all other frames are dropped.

Note: Make sure that the link used for managing the S3280 is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the S3280 via the serial interface.

Example:

```
>mac learning 1,2,3 secure
>mac learning

Port  Learning
----  -
1     Secure
2     Secure
3     Secure
4     Auto
5     Auto
6     Auto
7     Auto
8     Auto
>
```

Command: **MAC Dump**

Syntax: **mac dump** [<mac_max>] [<mac_addr>] [<vid>]

Description: Displays a sorted list of MAC address entries, where:
 <mac_max> : Maximum number of MAC addresses. The default is 'Show all' MAC addresses.
 <mac_addr>: First MAC address (xx-xx-xx-xx-xx-xx). The default is MAC address all zeros.
 <vid> : First VLAN ID (1-4094). The default is VID 1.

Example 1:

```
>mac dump
Type      VID  MAC Address          Ports
-----  ---  -
Static 1    00-00-00-00-00-00  2-4
Static 1    00-c0-f2-21-b8-c4  None, CPU
Static 1    33-33-00-00-00-01  1-6, 8, 9, CPU
Static 1    33-33-00-00-00-02  1-6, 8, 9, CPU
Static 1    33-33-ff-00-02-01  1-6, 8, 9, CPU
Static 1    33-33-ff-21-b8-c4  1-6, 8, 9, CPU
Static 1    ff-ff-ff-ff-ff-ff  1-9, CPU
>
```

Example 2:

```
>mac dump
Type      VID  MAC Address          Ports
-----  ---  -
Dynamic 1    00-04-75-bd-9c-36  1
Static 1    00-c0-f2-21-b8-c4  None, CPU
Dynamic 1    00-c0-f2-56-0a-44  5
Static 1    01-00-0c-cc-cc-cc  None, CPU
Static 1    33-33-00-00-00-01  1-6, 8-10, CPU
Static 1    33-33-00-00-00-02  1-6, 8-10, CPU
Static 1    33-33-ff-00-02-01  1-6, 8-10, CPU
Static 1    33-33-ff-21-b8-c4  1-6, 8-10, CPU
Static 1    ff-ff-ff-ff-ff-ff  1-10, CPU
>
```

Command: **MAC Statistics**

Syntax: **mac statistics** [<port_list>]

Description: Displays the MAC address table statistics for a specified S3280 port or for all ports, where:
 <port_list>: Port list or 'All'. The default is 'All' ports.

Example:

```
>mac statistics
Port  Dynamic Addresses
-----
1      181
2      0
3      0
4      0
5      0
6      0
7      0
8      0

Total Dynamic Addresses: 181
Total Static Addresses : 4
>mac statistics 1
Port  Dynamic Addresses
-----
1      181

Total Dynamic Addresses: 181
Total Static Addresses : 4
>
```

Command: **MAC Flush**

Syntax: **mac flush**

Description: Flush (delete) all learned entries from the MAC address table.

Example:

```
>mac flush
>mac statistics
Port  Dynamic Addresses
-----
1      0
2      0
3      0
4      0
5      0
6      0
7      0
8      0

Total Dynamic Addresses: 0
Total Static Addresses : 6
```

VLAN Management Port (MPort) PortType Command

Management VLAN is used for managing the switch from a remote location using a protocol such as telnet, SSH, or SNMP. Normally, the Management VLAN is VLAN 1, but you can configure any VLAN as the Management VLAN. TN recommends not using VLAN 1, and also not to use any VLAN that carries user data traffic as Management VLAN. You must configure IP address and default gateway for Management VLAN. After configuring IP address and default gateway for Management VLAN, you can telnet or SSH to the switch to perform switch management functions.

Note: Be sure to set the Management VLAN configuration before you set the VLAN configuration (using the VLAN commands in the section below).

Command: Set or Show the VLAN Management port PortType

Syntax: `vlan mport porttype [<port_list>] [unaware|c-port|s-port|s-custom-port]`

Description: Set or Show the VLAN Management port PortType, where:
[<port_list>] Port list or 'All'. The default is 'All' ports (1-8).

Type = [unaware|c-port|s-port|s-custom-port], where:

unaware: the port does not recognize VLANs. All frames are classified to the Port VLAN ID and tags are not removed. This means that MAC addresses are learned in VLAN 1, and the S3280 does not remove or insert VLAN tags. This is the default.

c-port: the port is a Customer port (C-port) with Customer tags (C-Tags), which use TPID 0x8100.

s-port: the port is a Service port (S-port) with Service tags (S-Tags), which use TPID 0x88A8 (IEEE 802.1ad).

s-custom-port: the port is a Custom Service port (S-custom-port) with Service tags (S-Tags), which use a custom TPID assigned in the S3280 firmware.

```
Example: >vlan mport porttype
Management Port PortType : Unaware

>vlan mport porttype c-port
>vlan mport porttype
Management Port PortType : C-Port

>vlan mport porttype s-port
>vlan mport porttype
Management Port PortType : S-Port

>vlan mport porttype s-custom-port
>vlan mport porttype
Management Port PortType : S-Custom-Port

>
```


VLAN Commands

VLAN (Virtual LAN) is a method used to restrict communication between S3280 ports. VLANs can be used with:

VLAN unaware switching is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the S3280 does not remove or insert VLAN tags.

VLAN aware switching is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

These S3280 commands provide Virtual LAN (VLAN) functions:

>**vlan ?**

Available Commands:

```

VLAN Configuration [<port_list>]
VLAN Translation Add <group_id> <vid> <trans_vid>
VLAN PVID [<port_list>] [<vid>|none]
VLAN Translation Delete <group_id> <vid>
VLAN FrameType [<port_list>] [all|tagged|untagged]
VLAN Translation Group [<port_list>] [<group_id>]
VLAN IngressFilter [<port_list>] [enable|disable]
VLAN tx_tag [<port_list>] [untag_pvid|untag_all|tag_all]
VLAN PortType [<port_list>] [unaware|c-port|s-port|s-custom-port]
VLAN MPort PortType [<port_list>] [unaware|c-port|s-port|s-custom-port]
VLAN remove <vid>|<name> [<port_list>]
VLAN EtypeCustomSport [<etype>]
VLAN Add <vid>|<name> [<port_list>]
VLAN Forbidden Add <vid>|<name> [<port_list>]
VLAN Delete <vid>|<name>
VLAN Forbidden Delete <vid>|<name>
VLAN Forbidden Lookup [<vid>] [(name <name>)]
VLAN Lookup [<vid>] [(name <name>)] [combined|static|nas|mvr|evc|all]
VLAN Name Add <name> <vid>
VLAN Name Delete <name>
VLAN Name Lookup [<name>]
VLAN Status [<port_list>] [combined|static|nas|mvr|mstp|erps|mep|vcl|all|conflicts]
>

```

Note: Be sure to set the Management VLAN configuration (previous section) before you set the VLAN configuration (this section).

Command: VLAN Configuration

Syntax: `vlan configuration` [<port_list>]

Description: Displays the current VLAN configuration, where:
<port_list>: Port list or 'all', default: All ports.

The VLAN Configuration example below shows the S3280 default VLAN configuration.

Example 1: `>vlan config`

```
VLAN Configuration:
=====

Port   PVID   Frame Type   Ingress Filter   Tx Tag           Port Type
-----
1      1      All          Disabled         Untag PVID       Unaware
2      1      All          Disabled         Untag PVID       Unaware
3      1      All          Disabled         Untag PVID       Unaware
4      1      All          Disabled         Untag PVID       Unaware
5      1      All          Disabled         Untag PVID       Unaware
6      1      All          Disabled         Untag PVID       Unaware
7      1      All          Disabled         Untag PVID       Unaware
8      1      All          Disabled         Untag PVID       Unaware

VID    VLAN Name           Ports
-----
1      default             1-9
444    Engineering         1-4
445    Marketing           4-7
446    Sales               2,5,8
447    Manufacturing       1,7,8

VLAN forbidden port list:
=====

VID    VLAN Name           Ports
-----
445    Marketing           3
446    Sales               1
>
```

The VLAN Configuration example below shows a more complex VLAN configuration with multiple VLANs configured with various Frame Types, TX Tagging, Port Type, and Forbidden Port settings.

Example 2:

```
>vlan config
VLAN Configuration:
=====

Port  PVID  Frame Type  Ingress Filter  Tx Tag  Port Type
-----
1      1      All         Disabled        Untag All  C-Port
2      None   Tagged      Disabled        Tag All   S-Port
3      1      Untagged   Disabled        Tag All   S-Custom-Port
4      1      All         Disabled        Untag PVID Unaware
5      1      All         Disabled        Untag PVID Unaware
6      1      All         Disabled        Untag PVID Unaware
7      1      All         Disabled        Untag PVID Unaware
8      1      All         Disabled        Untag PVID Unaware

VID    VLAN Name  Ports
-----
1      default    1,3-8
10     v10        2
11     v11        2
12     v12        2
13     v13        2
14     v14        2
15     v15        2
16     v16        2
17     v17        2
18     v18        2
19     v19        2
20     v20        2

VLAN forbidden port list:
=====

VID    VLAN Name  Ports
-----
1      default    2
>
```

Command:

Add VLAN Translation Entry

Syntax:

vlan translation add <group_id> <vid> <trans_vid>

Description:

Add VLAN translation entry into a group. The parameters are:

<group_id> : Group ID (1 to VTSS_PORTS) to which this entry will be added.

<vid> : VLAN ID (1-4094) to which this entry will be added.

<trans_vid>: Translation VLAN ID to which this entry will be added.

Example:

```
>VLAN Translation Add 1 1 1
>
```

Command: Delete VLAN Translation Group Entry

Syntax: `vlan translation delete <group_id> <vid>`

Description: Delete an existing VLAN translation entry from a group, where:
<group_id>: Group ID (1 to 8) of the entry to be deleted.
<vid>: VLAN ID (1-4094) of the entry to be deleted.

Example:

```
>vlan translation delete 1 1
>vlan translation group
Ports                                     Group ID
-----                                     -
```

1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8

```
>
```

Messages: No port members for VLAN "vid". Please check the delete button to delete VLAN from the list or add the members.

Command: Display VLAN Translation Group

Syntax: `vlan translation group [<port_list>] [<group_id>]`

Description: Display or map VLAN Translation Group configuration.

If only **port_list** is entered, displays the Port-to-Group mapping for each port.

If only **group_id** is entered, displays the VLAN Translations of that group.

If both **port_list** and **group_id** are entered, maps the ports in **port_list** to the **group** specified.

The parameters are:

<port_list>: Port list or 'all'. The default is 'All' ports.

<group_id>: Group ID (1 to 8).

Example:

```
>vlan translation group 1 8
>vlan translation group
Ports                                     Group ID
-----                                     -
```

2	2
3	3
4	4
5	5
6	6
7	7
1, 8	8

```
>
```

Command: VLAN PVID

Syntax: `vlan pvid [<port_list>] [<vid>|none]`

Description: Set or show the Port VLAN ID (PVID) , where:

<port_list>: Port list or 'All'. The default is 'All' ports.

<vid>|none : Port VLAN ID (1-4094) or 'none'. The default is 'Show port VLAN ID'.

This command configures the VLAN identifier for the port. The valid values are 1 - 4094.

The default is 1. Note that the port must be a member of the same VLAN as the Port VLAN ID.

Example:

```
>vlan pvid all

Port  PVID
----  ----
1     1
2     1
3     1
4     1
5     1
6     1
7     1
8     1
>vlan pvid all 3 5
Invalid parameter: 5

Syntax:
VLAN PVID [<port_list>] [<vid>|none]
>vlan pvid 3 5
>vlan pvid all

Port  PVID
----  ----
1     1
2     1
3     5
4     1
5     1
6     1
7     1
8     1
>vlan pvid 4 none
>vlan pvid all

Port  PVID
----  ----
1     1
2     1
3     5
4     None
5     1
6     1
7     1
8     1
>
```

Command: **VLAN FrameType**

Syntax: **vlan frametype** [<port_list>] [all|tagged|untagged]

Description: Set or show the port VLAN frame type, where:
 <port_list>: Port list or 'All'. The default is 'All' ports.

all : Allow tagged and untagged frames.

tagged : Allow tagged frames only.

untagged : Allow untagged frames only.

(The default is Show accepted frame types'.)

This command tells the port to accept all frames or only tagged frames or only untagged frames.

This command affects VLAN ingress processing. If the port only accepts tagged frames, then untagged frames received on the port are discarded. The default is allow **all** tagged and untagged frames.

Example:

```
>vlan frametype

Port  Frame Type
----  -
1     All
2     All
3     All
4     All
5     All
6     All
7     All
8     All
>vlan frametype 1 tagged
>vlan frametype 2 untagged
>vlan frametype

Port  Frame Type
----  -
1     Tagged
2     Untagged
3     All
4     All
5     All
6     All
7     All
8     All
>
```

Command: VLAN Ingress Filter**Syntax:** `vlan ingressfilter [<port_list>] [enable|disable]`**Description:** Set or show the port VLAN ingress filter, where:
`<port_list>`: Port list or 'All'. The default is All ports.**enable** : Enable VLAN ingress filtering.**disable** : Disable VLAN ingress filtering.

(The default is 'Show VLAN ingress filtering'.)

This command affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded.

By default, ingress filtering is disabled.

Example: `>vlan ingressfilter 1,2,3 enable``>vlan ingressfilter`

Port	Ingress Filter
1	Enabled
2	Enabled
3	Enabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled

Command: VLAN TX Tagging**Syntax:** `vlan tx_tag [<port_list>] [untag_pvid|untag_all|tag_all]`**Description:** Set or show the port egress tagging, where:
`<port_list>`: Port list or 'all'. The default is 'All' ports.**Tx tag** : (Egress tagging).**untag_pvid** : All VLANs except pvid will be tagged.**untag_all** : All VLANs will be untagged.**tag_all** : All VLANs will be tagged.**Example:** `>vlan tx_tag 1,2,3 untag_pvid``>vlan tx_tag 4,5,6 untag_all``>vlan tx_tag 7,8 tag_all``>vlan tx_tag`

Port	Tx Tag
1	Untag PVID
2	Untag PVID
3	Untag PVID
4	Untag All
5	Untag All
6	Untag All
7	Tag All
8	Tag All

Command: VLAN Port Type

Syntax: `vlan porttype [<port_list>] [unaware|c-port|s-port|s-custom-port]`

Description: Set or show the VLAN Port Type, where:
 <port_list>: Port list or 'all', default: All ports.
 Port Type:

unaware: the port does not recognize VLANs. All frames are classified to the Port VLAN ID and tags are not removed. This means that MAC addresses are learned in VLAN 1, and the S3280 does not remove or insert VLAN tags. This is the default.

c-port: the port is a Customer port (C-port) with Customer tags (C-Tags), which use TPID 0x8100.

s-port: the port is a Service port (S-port) with Service tags (S-Tags), which use TPID 0x88A8 (IEEE 802.1ad).

s-custom-port: the port is a Custom Service port (S-custom-port) with Service tags (S-Tags), which use a custom TPID assigned in the S3280 firmware.

Example:

```
>vlan porttype
Port  Port Type
----  -
1     Unaware
2     Unaware
3     Unaware
4     Unaware
5     Unaware
6     Unaware
7     Unaware
8     Unaware
>vlan porttype 1,2,3 c-port
>vlan porttype 4,5,6 s-port
>vlan porttype 7,8 s-custom-port
>vlan porttype
Port  Port Type
----  -
1     C-Port
2     C-Port
3     C-Port
4     S-Port
5     S-Port
6     S-Port
7     S-Custom-Port
8     S-Custom-Port
>
```


Command: Remove VLAN Entry

Syntax: `vlan remove <vid>|<name> [<port_list>]`

Description: Remove one or more ports in a VLAN entry, where:
 <vid>|<name>: VLAN ID (1-4094) or VLAN Name.
 <port_list> : Port list or 'All'. The default is 'All' ports.

Example:

```
>vlan lookup
VID      VLAN Name      Ports
-----
1        default        1-9
10       vid10           8
20       vid20           3-5
100      vid100          6,7
200      vid200          1,2
1000
>vlan remove 1 9
Invalid parameter: 9

Syntax:
VLAN remove <vid>|<name> [<port_list>]
>vlan remove 100 7
>vlan lookup
VID      VLAN Name      Ports
-----
1        default        1-9
10       vid10           8
20       vid20           3-5
100      vid100          1-6,8,9
200      vid200          1,2
1000
>
```

Command: VLAN Etype Custom S-port

Syntax: `vlan etypecustomsport [<etype>]`

Description: Set or show the Custom S-port EtherType, where:
Ether Type: enter a valid Ether Type in the range of 0x0600 - 0xFFFF.
 This parameter specifies the Ether type used for Custom S-ports. This is a global setting for all of the Custom S-ports.

Example:

```
>vlan etypecustomsport
TPID is 0x88a8
>vlan etypecustomsport 0x088a
>vlan etypecustomsport
TPID is 0x88a
>vlan etypecustomsport 0x0900
>vlan etypecustomsport
TPID is 0x900
>
```

Command: VLAN Add**Syntax:** **vlan add** <vid>|<name> [<port_list>]**Description:** Add or modify VLAN entry, where:
<vid>|<name>: VLAN ID (1-4094) or VLAN Name.
<port_list> : Port list or 'All'. The default is All ports.**Example:**
>**vlan add 1 1,2,3,4,5**
>**vlan add 2 6,7,8,9**
>**Command: VLAN Delete****Syntax:** **vlan delete** <vid>|<name>**Description:** Delete an existing VLAN entry, where:
<vid>|<name>: VLAN ID (1-4094) or VLAN Name.**Example:**
>**vlan delete 2**
>**vlan delete 2**
VLAN deletion failure**Command: VLAN Lookup****Syntax:** **vlan lookup** [<vid>] [(name <name>)] [combined|static|nas|mvr||voice_vlan|evc|all]**Description:** Lookup an existing VLAN entry, where:
<vid> : VLAN ID (1-4094), default: Show all VLANs.
name : VLAN name string.
<name>: VLAN name - Maximum of 32 characters. The VLAN Name can only contain alpha or numeric characters, including at least one alphabetic character.
combined : Shows All the Combined VLAN database entries.
static : Shows the VLAN entries configured by the administrator. With a Static VLAN (or "port-based" VLAN), assignments are created by assigning ports to a VLAN. As a device enters the network, the device automatically assumes the VLAN of the port. If you change ports and need access to the same VLAN, the network administrator must manually make a port-to-VLAN assignment for the new connection.
nas : Shows the VLANs configured by NAS (network access server).
mvr : Shows the VLANs configured by MVR (Multicast VLAN Registration).
evc : Shows the VLANs configured by EVCs.
all : Shows all VLANs configuration.
(The default is 'combined VLAN Users configuration'.)**Example:**
>**vlan lookup**
VID VLAN Name Ports

1 default 1-5
2 VID2 6-7
3 VID3 8-9
>

Command: **VLAN Forbidden Add**

Syntax: **vlan forbidden add** <vid>|<name> [<port_list>]

Description: Add a new or modify an existing VLAN entry in the forbidden table. The **vlan forbidden add** command modifies the list of forbidden ports assigned to a VLAN. Ports in this forbidden list will be forbidden (blocked) from using this VLAN. The parameters are:

<vid>|<name>: VLAN ID (1-4094) or VLAN Name.

<port_list> : Port list or 'all'. The default is 'All' ports.

Example:

```
>vlan forbidden add 4 4
>vlan forbidden lookup

VLAN forbidden port list:
=====

VID      VLAN Name          Ports
-----  -
4                4,9
>
```

Command: **VLAN Forbidden Delete**

Syntax: **vlan forbidden delete** <vid>|<name>

Description: Delete an existing VLAN entry from the forbidden table. The parameters are:

<vid>|<name>: VLAN ID (1-4094) or VLAN Name to be deleted.

Example:

```
>vlan forbidden lookup

VLAN forbidden port list:
=====

VID      VLAN Name          Ports
-----  -
4                4,9
>vlan forbidden delete 4
>vlan forbidden lookup

VID      VLAN Name          Ports
-----  -
VLAN forbidden table is empty
>
```

Command: **VLAN Forbidden Lookup**

Syntax: **vlan forbidden lookup** [<vid>] [(name <name>)]

Description: Display the existing VLAN Forbidden port table. The parameters are:

<vid> : VLAN ID (1-4094), default: Show all VLANs

name : VLAN name string

<name>: VLAN name - Maximum of 32 characters. The VLAN Name can only contain alpha or numeric characters. The VLAN name should contain at least one alpha character.

Example: >**vlan forbidden lookup**

```

VID      VLAN Name                               Ports
-----  -
VLAN forbidden table is empty
>vlan forbidden add 4 4
>vlan forbidden lookup

VLAN forbidden port list:
=====

VID      VLAN Name                               Ports
-----  -
4        4,9
>
```

Command: **VLAN Name Add**

Syntax: **vlan name add** <name> <vid>

Description: Add a new VLAN Name to an existing VLAN ID mapping, where:

<name>: Enter a VLAN name with a maximum of 32 characters. The 'VLAN Name' can only contain alpha or numeric characters, and must include at least one alphabetic character.

<vid> : VLAN ID (1-4094) to be added.

Example: >**vlan name add VID2 2**
>**vlan name add VID3 3**
>**vlan name add VID4 4**
>

Command: **VLAN Name Delete**

Syntax: **vlan name delete** <name>

Description: Delete a VLAN Name from VLAN ID Mapping, where:

<name>: VLAN name with a maximum of 32 characters. The 'VLAN Name' can only contain alpha or numeric characters, and must include at least one alphabetic character.

Example: >**vlan name delete VID2**
>**vlan name delete VID3**
>

Command: **VLAN Name Lookup**

Syntax: **vlan name lookup** [<name>]

Description: Show (display) the current VLAN Name table, where:
 <name>: VLAN name with a maximum of 32 characters. The 'VLAN Name' can only contain alpha or numeric characters, and must include at least one alpha character.

Example:

```
>vlan name lookup
VLAN NAME                               vid
-----
default                                  1
VID4                                       4
>
```

Command: **Remove Ports from VLAN entries**

Syntax: **vlan remove** <vid>|<name> [<port_list>]

Description: Remove one or more existing ports in VLAN entry. This will effectively remove ports (VLAN entries) from the VID list. You can use this command to exclude the S3280 MGMT port from a newly configured VLAN. The parameters are:

<vid>|<name>: VLAN ID (1-4094) or VLAN Name.

<port_list> : Port list or 'All'. The default is 'All' ports.

Example:

```
>vlan lookup
VID   VLAN Name                               Ports
-----
1     default                                  1-9
10    vid10                                       8
20    vid20                                       3-5
100   vid100                                      1-6, 8, 9
200   vid200                                      1, 2
1000  3

>vlan remove 100 8
>vlan lookup
VID   VLAN Name                               Ports
-----
1     default                                  1-9
10    vid10                                       8
20    vid20                                       3-5
100   vid100                                      1-7, 9
200   vid200                                      1, 2
1000  3
>
```

Command: VLAN Status

Syntax: **vlan status** [<port_list>] [combined|static|nas|mvr|voice_vlan|mstp|erps|mep|vcl|all|conflicts]

Description: Display the current VLAN Port Configuration status, where:

<port_list>: Port list or 'All'. The default is 'All' ports.

combined : show all VLAN User configurations (i.e., all of the types listed below).

static : show just static port configuration. With a Static VLAN ("port-based" VLAN), assignments are created by assigning ports to a VLAN. As a device enters the network, the device automatically assumes the VLAN of the port. If you change ports and need access to the same VLAN, the network administrator must manually make a port-to-VLAN assignment for the new connection.

nas : show just NAS port configuration (network access server).

mvr : show just MVR port configuration (Multicast VLAN Registration).

mstp : show just MSTP port configuration.

erps : show just ERPS port configuration.

mep : show just MEP port configuration.

vcl : show just VCL (VLAN Control List) port configuration.

all : show All VLAN Users configuration (default: all VLAN Users configuration).

Example 1:

>**vlan status 1-6**

Port	VLAN User	PortType	PVID	Frame Type	Ing Filter	Tx Tag	UVID	Conflicts
1	Static	Unaware	1	All	Disabled	Untag This	1	MSTP No ERPS No MEP No EVC No
2	Combined Static	Unaware Unaware	1 1	All All	Disabled Disabled	Untag This Untag This	1 1	MSTP No ERPS No MEP No EVC No
3	Combined Static	Unaware Unaware	1 1	All All	Disabled Disabled	Untag This Untag This	1 1	MSTP No ERPS No MEP No EVC No
4	Combined Static	Unaware Unaware	1 1	All All	Disabled Disabled Enabled	Untag This Untag All	1 1	MSTP No ERPS No MEP No EVC No
5	Combined Static	Unaware Unaware	1 1	All All	Enabled Disabled	Untag All Untag All	4096 1	MSTP No ERPS No MEP No EVC No
6	Combined Static	Unaware Unaware	1 1	All All	Disabled Disabled	Untag All Untag All	4096 1	MSTP No ERPS No MEP No EVC No
	Combined	Unaware	1	All	Disabled	Untag All	4096	No

Example 2:

```
>vlan status combined
```

Port	PortType	PVID	Frame Type	Ing Filter	Tx Tag	UVID	Conflicts
1	Unaware	1	All	Enabled	Untag This	1	No
2	Unaware	1	All	Enabled	Untag This	1	No
3	Unaware	1	All	Enabled	Untag All	4096	No
4	Unaware	1	All	Disabled	Untag This	1	No
5	C-Port	1	All	Disabled	Tag This	1	No
6	Unaware	1	All	Disabled	Untag This	1	No
7	Unaware	1	All	Disabled	Untag This	1	No
8	Unaware	1	All	Disabled	Untag This	1	No

The reported fields are:

Port: The logical port for the settings contained in the same row.

Port Type: Shows the Port Type. Port type can be any of Unaware, C-port, S-port, Custom S-port.

If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed.

C-port is Customer Port. S-port is Service port. Custom S-port is S-port with Custom TPID.

PVID: Shows the VLAN identifier for that port. The allowed values are 1 through 4094. The default value is 1.

Frame Type: Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.

Ing Filter: Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.

Tx Tag: Shows egress filtering frame status whether tagged or untagged.

UVID: Shows the UVID (untagged VLAN ID). A Port's UVID determines the packet's behaviour at the egress side.

Conflicts: Shows whether Conflicts exists or not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, these conflicts can occur:

- Functional Conflicts between features.
- Conflicts due to hardware limitation.
- Direct conflict between user modules.

VID (VLAN ID) Range Summary

Some S3280 modules accept VID range 0 – 4094 and some modules only accept VID range 1 – 4094. A VID of 0 is only for modules where untagged/priority tag makes sense. LLDP and LOAM are untagged. The valid VID ranges are summarized below.

<u>Module</u>	<u>Valid VID Range</u>
ACL	(1-4094)
ARP Inspection	(1-4094)
ERPS	(1-4094)
EVC	
1. EVC parameters:	1) VID (1-4094), 2) IVID(1-4094)
	Inner Tag-->VLAN ID (0-4094)
	Outer Tag-->VLAN ID (0-4094)
2. ECEs > UNI Matching > VLAN ID Value	(0-4094)
IP (Management VLAN)	(1 -4094)
IP Source Guard	(1 - 4094)
IPMC	(1-4094) (only up to VLANs)
LLDP	(none)
MAC	(1-4094)
MEP UP	(1-4094) {depends on the VLANs}
MEP Down	(0-4094)
MVR	(1-4094)
PTP	(0-4094)
QOS (QCL)	(1-4094)
VCL	(1-4094)
VLAN translation	(1-4094)

PVLAN Commands

An S3280 VLAN can be configured as a Private VLAN (PVLAN). In a private VLAN, PVLANS provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

PVLAN commands let you:

- Configure, modify, and view Private VLAN membership configurations,
- Add or delete Private VLANs, and
- Add or remove Port members of each Private VLAN.

Private VLANs are based on the source port mask, and they have no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

These S3280 commands provide Private Virtual LAN (PVLAN) functions:

>**pvlan ?**

Available Commands:

PVLAN Configuration [<port_list>]
PVLAN Add <pvlan_id> [<port_list>]
PVLAN Delete <pvlan_id>
PVLAN Lookup [<pvlan_id>]
PVLAN Isolate [<port_list>] [enable|disable]
 >

The S3280 PVLAN commands are explained below.

Command: **Configure PVLAN**

Syntax: **pvlan configuration** [<port_list>]

Description: Show the current Private VLAN configuration, where:
 <port_list>: Port list or 'All'. The default is 'All' ports.

Example: >**pvlan config**
 Private VLAN Configuration:
 =====
 Port Isolation
 ---- -
 1 Disabled
 2 Disabled
 3 Disabled
 4 Disabled
 5 Disabled
 6 Disabled
 7 Enabled
 8 Disabled

 PVLAN ID Ports
 ----- -
 1 1-8
 3 1, 3, 5
 >

Command: Add PVLAN**Syntax:** `pvlan add <pvlan_id> [<port_list>]`**Description:** Add a new or modify an existing Private VLAN entry, where:`<pvlan_id>` : Private VLAN ID. The allowed range for a Private VLAN ID is the same as the S3280 port number range.`<port_list>`: Port list or 'all', default: All ports.

Example:

```
>pvlan add 1 1,2
>pvlan add 2 2,3,4,5,6
>
```

Command: Delete PVLAN**Syntax:** `pvlan delete <pvlan_id>`**Description:** Delete an existing Private VLAN entry, where:`<pvlan_id>`: Private VLAN ID. The allowed range for a Private VLAN ID is the same as the S3280 port number range.

Example:

```
>pvlan delete 1
>
```

Command: Isolate PVLAN**Syntax:** `pvlan isolate [<port_list>] [enable|disable]`**Description:** Set or show the port isolation mode, where:`<port_list>`: Port list or 'all', default: All ports.**enable** : Enable port isolation.**disable** : Disable port isolation.

(default: Show port isolation port list)

Example:

```
>pvlan isolate

Port  Isolation
----  -
1     Disabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
>pvlan isolate 2,3,4 enable
>pvlan isolate

Port  Isolation
----  -
1     Disabled
2     Enabled
3     Enabled
4     Enabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
>
```

Command: **Lookup PVLAN**

Syntax: **pvlan lookup** [<pvlan_id>]

Description: Lookup Private VLAN entry, where:

<**pvlan_id**>: Private VLAN ID, default: Show all PVLANS. The allowed range for a Private VLAN ID is the same as the S3280 port number range (1-8).

Example: >**pvlan lookup**

```
PVLAN ID  Ports
-----  -
1         1-8
>pvlan add 2 2-6
>pvlan lookup

PVLAN ID  Ports
-----  -
1         1-8
2         2-6
>
```

Security Commands

These S3280 commands provide a wide range of Security management functions, including Switch, Network, and AAA (Authentication, Authorization and Accounting) subgroups. The Security command group includes these sub-groups:

>**security ?**

Command Groups:

Switch: Switch security

Network: Network security

AAA: Authentication, Authorization and Accounting

Each of these sub-groups contains underlying commands and/or command groups.

Security Switch Commands

The **Security Switch** group commands include these command subgroups:

Security Switch Users : User management

Security Switch Privilege: Privilege level

Security Switch Auth : Authentication

Security Switch SSH : Secure Shell

Security Switch HTTPS : Hypertext Transfer Protocol over Secure Socket Layer

Security Switch Access : Access management

Security Switch SNMP : Simple Network Management Protocol

Security Switch RMON : Remote Network Monitoring

These subgroups' commands are explained in the following sections.

Security Switch Users Group Commands

These commands let you display the current set of users and add users to and delete users from the list.

Command: **Security Switch Users Configuration**

Syntax: **security switch users config**

Description: Show current users configuration.

Example: **>security switch users config**

```
Users Configuration:
=====

User Name                Privilege Level
-----
admin                    15
jeffs                    2
```

Command: Add Security Switch Users**Syntax:** **security switch users add** <user_name> <password> <privilege_level>

Description: Add a new user or modify an existing user's name, password or privilege level, where:

<user_name> : A string identifying the user name that this entry should belong to. The allowed string length is (1-32). The valid user name is a combination of letters, numbers and underscores. The change is immediately effective, and you do not need to know the old password. Note that a level 1 user can view the full set of help commands, but if you enter "security", an 'invalid command' message is returned.

<password> : The password for this user name. The allowed string length is (0-32). Use 'clear' or "" as null string.

<privilege_level>: User privilege level (1-15). See the "security switch privilege level config" command for details.

Example:

```
>security switch users config

Users Configuration:
=====

User Name                               Privilege Level
-----                               -
admin                                     15
>security switch users add jeffs Buffrey1 2
>security switch users config

Users Configuration:
=====

User Name                               Privilege Level
-----                               -
admin                                     15
jeffs                                     2
>
```

Command: Delete Security Switch Users

Syntax: security switch users delete <user_name>

Description: Delete users entry, where:

<user_name>: A string identifying the user name that this entry should belong to. The allowed string length is (1-32). The valid user name is a combination of letters, numbers and underscores.

```
Example: >security switch users config

Users Configuration:
=====

User Name                               Privilege Level
-----
admin                                     15
jeffs                                     2
>security switch users delete jeffs
>security switch users config

Users Configuration:
=====

User Name                               Privilege Level
-----
admin                                     15
>
```

Security Switch Privilege Group Commands

These commands let you display and configure the user privilege levels. The valid range is 1 to 15. If the privilege level value is 15, it can access all groups (i.e. it is granted full control of the device). But others values need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level in order to have the access of that group. By default, most groups have privilege level 5 with read-only access; privilege level 10 has read-write access. The system maintenance functions (software upload, factory defaults and etc.) require user privilege level 15.

Generally, the user privilege levels are:

- Privilege Level 15 can be used for an Administrator account,
- Privilege Level 10 for a Standard (basic) user account, and
- Privilege Level 5 for a Guest account.

Notes on Security Switch Privilege Levels

1. Levels 1 – 4 display the same help information and support only 7 commands. These are all inquiry actions that cannot change the S3280 in any way. While more detailed help levels show only these commands available, the main help screen is unchanged and shows all of the main command groups that the other levels show. This level can do only these commands according to help: Help, Logout, Port Configuration, Port DMI Statistics, Port SFP, Port Statistics, and Up.
2. In addition: usually, entering a single letter followed by question mark should list all the commands that start with that letter. At level 1, entering “s ?” yields output which looks inconsistent with related privilege level commands.
3. Levels 5 – 9 display the same help information and support 392 commands.
4. Levels 10 and 12 - 14 display the same help information and support 490 commands. Level 11 displays the same information as levels 1 – 4.
5. Level 15 supports 656 commands. Level 15 adds Firmware commands and the Security Switch Privilege Level Configuration / Current, Security Switch Users Add / Configuration / Delete, and System Reboot command support.
6. Only a level 15 user can display the current security level.

The Security Switch Privilege Group Commands are listed below.

>security switch priv ?

Available Commands:

Security Switch Privilege Level Configuration

Security Switch Privilege Level Group <group_name> [<cro>] [<crw>] [<sro>] [<srw>]

Security Switch Privilege Level Current

Note that by changing to a lower privilege level you may lock yourself out of S3280 CLI access.

Command: **Show Current Privilege Level**

Syntax: **security switch priv level current**

Description: Displays the current privilege level.

Example: >**security switch priv level current**
Privilege Current Level: 15

Command: Show Current Privilege Level Configuration

Syntax: security switch privilege level config

Description: Displays the current privilege configuration, where:

<group_name>: Privilege group name

<cro> : Configuration read-only privilege level (1-15).

<crw> : Configuration/Execute read-write privilege level (1-15).

<sro> : Status/Statistics read-only privilege level (1-15).

<srw> : Status/Statistics read-write privilege level (1-15).

Example: >security switch privilege level config

```
Privilege Level Configuration:
=====
```

```
Privilege Current Level: 15
```

Group Name,	MODULE_ID, MODULE_ID	Privilege Level			
		CRO	CRW	SRO	SRW
Aggregation		19	5	10	5 10
Diagnostics		27	5	10	5 10
EPS		45	5	10	5 10
ERPS		72	5	10	5 10
ETHER_SAT		194	5	10	5 10
ETH_LINK_OAM		73	5	10	5 10
EVC		62	5	10	5 10
IP		18	5	10	5 10
IPMC_LIB		94	5	10	5 10
IPMC_Snooping		82	5	10	5 10
LACP		35	5	10	5 10
LLDP		34	5	10	5 10
Loop_Protect		91	5	10	5 10
MAC_Table		12	5	10	5 10
MEP		46	5	10	5 10
MVR		69	5	10	5 10
Maintenance		16	15	15	15 15
Mirroring		15	5	10	5 10
PHY		97	5	10	5 10
PTP		65	5	10	5 10
Port_Security		66	5	10	5 10
Ports		11	5	10	1 10
Private_VLANS		23	5	10	5 10
QoS		14	5	10	5 10
SNMP		36	5	10	5 10
Security		60	5	10	5 10
Spanning_Tree		20	5	10	5 10
Static_Routing		197	5	10	5 10
System		24	5	10	1 10
Timer		93	5	10	5 10
VCL		79	5	10	5 10
VLAN_Translation		85	5	10	5 10
VLANs		13	5	10	5 10
sFlow		83	5	10	5 10

Note: The S32880-TST models have **EtherSAT Loopback** commands and **Firmware Peripheral** commands that the S3280 does not support.

Message: Must explicitly add case for module ID: %d

Meaning: A user privilege_level was not defined for a module.

Recovery: 1. You must define a privilege level for the module (e.g., crw = 10).

Command: **Configure Privilege Level Group**
Syntax: **security switch privilege level group** <group_name> [<cro>] [<crw>] [<sro>] [<srw>]
Description: Configure a privilege level group, where:
 <group_name>: Privilege group name.
 <cro> : Configuration read-only privilege level (1-15).
 <crw> : Configuration/Execute read-write privilege level (1-15).
 <sro> : Status/Statistics read-only privilege level (1-15).
 <srw> : Status/Statistics read-write privilege level (1-15).

Example:

```
>security switch privilege level group QoS
Group Name                               Privilege Level
                                           CRO CRW SRO SRW
-----
QoS                                       5  10  5  10
>security switch privilege level group QoS 6
>security switch privilege level group QoS
Group Name                               Privilege Level
                                           CRO CRW SRO SRW
-----
QoS                                       6  10  5  10
>
```

Messages:

Invalid <group_name> parameter: grp1

The privilege level of 'Read-only' should be less than or equal to 'Read-write'

Security Switch Auth Group Commands

Command: **Show Current Authentication Configuration**
Syntax: **security switch auth config**
Description: Show the current Authentication configuration.
Example: >security switch auth config

```
Auth Configuration:
=====
Client      Authentication Method      Local Authentication Fallback
-----
console     local                       Disabled
telnet      local                       Disabled
ssh         local                       Disabled
web         local                       Disabled
>
```

Command: Set Authentication Method**Syntax:** **security switch auth method** [console|telnet|ssh|web] [none|local] [enable|disable]**Description:** This command defines how a user is authenticated when they log into the S3280 via one of the management client interfaces. Set or show the S3280 Authentication method (default: Show Auth method), where:**console** : Settings for CONSOLE PORT access to the S3280.**telnet** : Settings for telnet access to the S3280.**ssh** : Settings for ssh access to the S3280.**web** : Settings for web access to the S3280.

(default: Set or show the specific client authentication method)

none : Authentication disabled; login is not possible.**local** : Use local authentication; use the local S3280 user database for authentication.**radius** : Use remote RADIUS authentication**tacacs+** : Use remote TACACS+ authentication

(The default is 'Show client authentication method'.)

enable : Enable local authentication if remote authentication fails.**disable** : Disable local authentication if remote authentication fails.*(Note: this parameter is effective as soon as it is typed.)***Example:** Security/Switch>**auth method ssh none disable**Security/Switch>**auth config**

Auth Configuration:

=====

Client Authentication Method

console local

telnet local

ssh none

web local

Security/Switch>

Security Switch SSH Group

Command: Show Current SSH Configuration

Syntax: security switch ssh configuration

Description: Show the current SSH configuration.

Example: Security/Switch>ssh config

```
SSH Configuration:
=====

SSH Mode : Enabled
Security/Switch>
```

Command: Set / Show SSH Mode

Syntax: security switch ssh mode [enable|disable]

Description: Set or show the current SSH mode, where:
enable : Enable SSH mode operation.
disable: Disable SSH mode operation.
(default: Show SSH mode)

Example: Security/Switch>ssh mode disable
Security/Switch>ssh mode
SSH Mode : Disabled
Security/Switch>

Security Switch HTTPS Group

Command: Show Current HTTPS Configuration

Syntax: security switch https configuration [enable|disable]

Description: Show the current HTTPS configuration.

Example: >security switch https config

```
HTTPS Configuration:
=====

HTTPS Mode           : Disabled
HTTPS Redirect Mode : Disabled
>
```

Command: Set / Show HTTPS Mode

Syntax: security switch https mode [enable|disable]

Description: Set or show the HTTPS mode, where:
enable : Enable HTTPS mode operation.
disable: Disable HTTPS mode operation.
(default: Show HTTPS mode)

Example: Security/Switch>https mode enable
Security/Switch>
Security/Switch>https mode
HTTPS Mode : Enabled
Security/Switch>

Command: Set / Show HTTPS Redirect

Syntax: **security switch https redirect** [enable|disable]

Description: Set or show the HTTPS redirect mode. When enabled, the S3280 automatically redirects the web browser to HTTPS when the HTTP prefix is entered, where:

enable : Enable HTTPS redirect

disable: Disable HTTPS redirect

(default: Show current HTTPS redirect mode)

Example:

```
Security/Switch>https redirect disable
Security/Switch>https redirect
HTTPS Redirect Mode : Disabled
Security/Switch>
```

Command: **Show HTTPS Certificate**

Syntax: **security switch https cert show**

Description: Displays the current HTTPS certificate information. The HTTPS Certificate validity period is from Jan. 1, 2010 to Dec. 31, 2029.

Example: >**security switch https cert show**

```
Certificate Information: (length: 1065)
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 2 (0x2)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: CN=S3280
    Validity
      Not Before: Jan  1 00:00:16 2010 GMT
      Not After  : Dec 31 00:00:16 2029 GMT
    Subject: CN=S3280
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (512 bit)
        Modulus (512 bit):
          00:d6:1b:74:a8:28:2c:0a:62:6a:1f:ed:40:43:ba:
          70:14:37:ff:f6:c0:d7:e0:ec:f3:1d:c1:86:0d:5f:
          09:2c:f5:25:82:8d:f5:77:ab:62:fc:34:25:a4:b0:
          bb:ba:21:c4:e0:46:c7:39:5f:12:ab:36:44:9e:b9:
          ba:73:72:2e:b3
        Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
    9e:7b:9c:bd:39:a1:b6:09:95:06:fe:7c:71:05:b9:4a:54:07:
    54:76:9a:0a:27:6e:a3:62:fa:5e:66:94:c6:ae:e1:4e:0c:61:
    74:99:1e:d0:be:db:68:49:29:ce:09:a6:6f:4b:86:f8:46:c2:
    de:1a:12:d8:ba:69:f7:8c:f0:f6
>
```

Messages:

>W web 08:14:26 53/handler_config_https_cert_load#258: Warning: SSL Certificate PEM file size too big

Command: Generate HTTPS Certificate**Syntax:** `security switch https certificate generate [rsa|dsa]`

Description: Generate a new HTTPS certificate. You must disable HTTPS mode before using this command (see the “**Security Switch HTTPS Mode**” command). The parameters are:
rsa : An algorithm which stands for Rivest, Shamir and Adleman who first publicly described it.
dsa: Digital Signature Algorithm.
 (default: RSA)

Example:

```
>security switch https certificate generate
Error: Please disable HTTPS mode first
>Security Switch HTTPS Mode disable
>security switch https certificate generate
>security switch https certificate generate dsa
>
```

Messages: *Error: Please disable HTTPS mode first*

Command: Load Security Switch HTTPS Certificate**Syntax:** `security switch https certificate load <hostname> <file_name>`

Description: Load a new HTTPS certificate from a TFTP server. The TFTP server must be configured and running in order to use this command. Also, you must disable HTTPS mode before running this command (see the `security switch https mode` command).

The parameters are:

<**hostname**> : IP Address or Hostname.

<**file_name**>: certificate file name (e.g., *S3280-cacert-key.pem*).

The certificate generated for use with the S3280 should be a *.pem* (Privacy Enhanced Mail) file containing both the certificate and the private key. The private key must be generated using `rsa_keygen_bits:512`.

Example:

```
>security switch https certificate load 192.168.1.30 S3280-cacert-key.pem
Error: Please disable HTTPS mode first
>security switch https mode
HTTPS Mode      : Enabled
>security switch https mode disable
>security switch https mode
HTTPS Mode      : Disabled
>security switch https certificate load 192.168.1.30 S3280-cacert-key.pem
>
```

Messages:

Error: File S3280-cacert-key was not found

Error: Please disable HTTPS mode first

Generate a Self-signed Certificate

A self signed certificate can be generated using openssl.

1. Type **openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:512 -out s3280-key.pem.**
2. Type **openssl req -key s3280-key.pem -x509 -new -set_serial 2 -days 3650 -out s3280-cacert.pem.**
3. Type **cat s3280-cacert.pem s3280-key.pem > s3280-cacert-key.pem.**

The extension is *.pem* by convention.

Load a Certificate from the CLI

1. Start and configure the TFTP server.
2. Place the certificate to load in your tftpboot root (e.g., *C:\TFTP-Root*) and run:

Security Switch HTTPS Certificate Load <ip-of-tftp-server> <cacert-key.pem>

Note: HTTPS Certificate Backup and Restore via the Web interface is different than via the CLI. The Web uses 'Form' upload and HTTP download, and the CLI uses TFTP.

Security Switch Access Group

Command: Show Security Switch Access Configuration
Syntax: security switch access configuration
Description: Display the current access management configuration.
Example:

```
>security switch access config

Access Mgmt Configuration:
=====

System Access Mode : Disabled
W: WEB/HTTPS
S: SNMP
T: TELNET/SSH

Idx Start IP Address           End IP Address                W S T
-----
>
```

Command: Set / Show Access Mode
Syntax: security switch access mode [enable|disable]
Description: Set or show the access management mode, where:
enable : Enable access management.
disable: Disable access management.
(default: Show access management mode)

Example:

```
>security switch access mode
System Access Mode : Disabled
>security switch access mode enable
>security switch access mode
System Access Mode : Enabled
>
```

Command: Add Access Entry
Syntax: security switch access add <access_id><start_ip_addr><end_ip_addr>[web][snmp][telnet]
Description: Add S3280 access management entry, default: Add all supported protocols, where:
<access_id> : entry index (1-16).
<start_ip_addr>: Starting IP address (a.b.c.d).
<end_ip_addr> : Ending IP address (a.b.c.d).
web : Indicates that the host can access the S3280 from HTTP/HTTPS.
snmp : Indicates that the host can access the S3280 from SNMP.
telnet : Indicates that the host can access the S3280 from TELNET/SSH.

Example:

```
>security switch access add 1 192.168.1.20 192.168.1.30 web snmp telnet
>
```

Note: use the **security switch access lookup** command to display the new entry.

Command: Add Ipv6 Access Entry

Syntax: **security switch access ipv6 add** <access_id> <start_ipv6_addr> <end_ipv6_addr> [web] [snmp] [telnet]

Description: Add a new access management IPv6 entry. The default is add all supported protocols. The parameters are:

<access_id> : entry index (1-16).

<start_ipv6_addr>: Starting IPv6 address.

IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon to separate each field (:).

For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once.

It also used a following a legal IPv4 address (e.g., '::192.1.2.34').

<end_ipv6_addr> : Ending IPv6 address.

IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon to separate each field (:).

For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once.

It also used a following a legal IPv4 address (e.g., '::192.1.2.34').

web : Indicates that the host can access the switch from HTTP/HTTPS.

snmp : Indicates that the host can access the switch from SNMP.

telnet : Indicates that the host can access the switch from TELNET/SSH.

Example:

```
>security switch access ipv6 add 1 fe80::215:c5ff:fe03:4dc7 fe80::215:c5ff:fe03:4fff web snmp telnet
>
```

Command: Delete Access Entry

Syntax: **security switch access delete** <access_id>

Description: Delete an existing access management entry, where:
<access_id>: entry index (1-16).

Example:

```
>security switch access delete 2
Non-existing entry ID 2
>security switch access delete 1
>
```

Command: Lookup (Display) Access Entry

Syntax: **security switch access lookup** [<access_id>]

Description: Lookup an existing access management entry, where:
<access_id>: entry index (1-16).

Example:

```
>security switch access lookup
```

W: WEB/HTTPS

S: SNMP

T: TELNET/SSH

Idx	Start IP Address	End IP Address	W	S	T
1	fe80::215:c5ff:fe03:4dc7	fe80::215:c5ff:fe03:4dc7	Y	Y	Y

```
>
```


Command: Clear Access Entry
Syntax: security switch access clear
Description: Clear access management entry.

Example:

```
>security switch access clear
>security switch access lookup
W: WEB/HTTPS
S: SNMP
T: TELNET/SSH

Idx Start IP Address                End IP Address                W S T
-----
>
```

Command: Show / Clear Access Statistics
Syntax: security switch access statistics [clear]
Description: Show or clear access management statistics, where:
clear: Clear the access management statistics.

Example:

```
>security switch access statistics clear
>security switch access statistics

Access Management Statistics:
-----
HTTP      Receive:      0    Allow:      0    Discard:    0
HTTPS     Receive:      0    Allow:      0    Discard:    0
SNMP      Receive:      0    Allow:      0    Discard:    0
TELNET    Receive:      0    Allow:      0    Discard:    0
SSH       Receive:      0    Allow:      0    Discard:    0
>
```

Security Switch RMON Group Commands

The S3280 Security Switch RMON (Remote Network Monitoring) commands let you add, delete or look up RMON statistics, history, alarms, and/or events.

The Security Switch RMON Group commands are explained below.

Command: Add RMON Statistics Entry

Syntax: `security switch rmon statistics add <stats_id> <data_source>`

Description: Add or modify an RMON Statistics entry. The entry index key is <stats_id>. Parameters are:
 <stats_id> : Statistics ID (1-65535).
 <data_source>: The OID (Object Identifier) that indicates that the ifIndex in ifEntry. The value should be something like .1.3.6.1.2.1.2.2.1.1.xxx.

Example:

```
>security switch rmon statistics add 1 .1.3.6.1.2.1.2.2.1.1.123
>
```

Messages: <data_source> dosen't exit

Command: Delete RMON Statistics Entry

Syntax: `security switch rmon statistics delete <stats_id>`

Description: Delete RMON Statistics entry. The entry index key is <stats_id>. The parameters are:
 <stats_id>: Statistics ID (1-65535).

Example:

```
>security switch rmon statistics delete 1
module_id=92, code=-6
>
```

Command: Lookup RMON Statistics Entries

Syntax: `security switch rmon statistics lookup [<stats_id>]`

Description: Show existing RMON Statistics entries, where:
 <stats_id>: Statistics ID (1-65535).

Example:

```
>security switch rmon statistics lookup
Id      Data Source          etherStatsOctets  etherStatsPkts  ether StatsCRCAlignErrors
-----
1       .1.3.6.1.2.1.2.2.1.1.1  43815621         676435         0

Number of entries: 1
>
```

Command: Add RMON History Entry

Syntax: `security switch rmon history add <history_id> <data_source> [<interval>] [<buckets>]`

Description: Add or modify RMON History entry. The entry index key is <history_id>. The parameters are:

<**history_id**> : History ID (1-65535).

<**data_source**>: The OID that indicates that the ifIndex in ifEntry. The value should be something like .1.3.6.1.2.1.2.2.1.1.xxx.

<**interval**> : Sampling interval (1-3600) (default: 1800).

<**buckets**> : The maximum data entries associated this History control entry stored in RMON (1-65535) (default: 50).

Example:

```
>security switch rmon history add 1 .1.3.6.1.2.1.2.2.1.1.987 1500 25
>
```

Messages: `<data_source> dosen't exit`

Command: Delete RMON History Entry

Syntax: `security switch rmon history delete <history_id>`

Description: Delete an RMON History entry. The entry index key is <history_id>. The parameters are:

<**history_id**>: History ID (1-65535).

Example:

```
>security switch rmon history delete 1
module_id=92, code=-7
>security switch rmon history delete 2
module_id=92, code=-7
```

Messages: `Invalid <history_id> parameter: 0
module_id=92, code=-7`

Command: **Lookup RMON History Entries**

Syntax: **security switch rmon history lookup** [<history_id>]

Description: Show RMON History entries (note that this can be a long display). The parameters are:
 <history_id>: History ID (1-65535) to be displayed.

```

Example: >security switch rmon history lookup 1
Entry Index           : 1
Data Source           : .1.3.6.1.2.1.2.2.1.1.1
Data Bucket Request   : 50
Data Bucket Granted   : 50
Data Interval         : 1800
etherHistorySampleIndex : 1
    etherHistoryIntervalStart : 0d 00:01:02 (62)
    etherHistoryDropEvents    : 0
    etherHistoryOctets        : 359293
    etherHistoryPkts          : 1740
    etherHistoryBroadcastPkts : 90
    etherHistoryMulticastPkts : 1324
    etherHistoryCRCAlignErrors: 0
    etherHistoryUndersizePkts : 0
    etherHistoryOversizePkts  : 0
    etherHistoryFragments     : 0
    etherHistoryJabbers       : 0
    etherHistoryCollisions    : 0
    etherHistoryUtilization    : 0
:      :      :      :      :
:      :      :      :      :
etherHistorySampleIndex : 34
    etherHistoryIntervalStart : 0d 16:30:00 (59400)
    etherHistoryDropEvents    : 0
    etherHistoryOctets        : 210439
    etherHistoryPkts          : 1372
    etherHistoryBroadcastPkts : 23
    etherHistoryMulticastPkts : 1312
    etherHistoryCRCAlignErrors: 0
    etherHistoryUndersizePkts : 0
    etherHistoryOversizePkts  : 0
    etherHistoryFragments     : 0
    etherHistoryJabbers       : 0
    etherHistoryCollisions    : 0
    etherHistoryUtilization    : 0
>

```

Command: Add / Modify RMON Alarm Entry

Syntax: security switch rmon alarm add <alarm_id> <interval> <alarm_variable> [absolute|delta]
<rising_threshold> <rising_event_index> <falling_threshold> <falling_event_index>
[rising|falling|both]

Description: Add or modify an RMON Alarm entry. The entry index key is <alarm_id>. The parameters are:

<alarm_id> : Alarm ID (1-65535).

<interval> : Sampling interval (1-2147483647) (default: 30).

<alarm_variable> : The MIB OID that must be referenced. Enter a variable value in the format xxx.yyy, where xxx is 10-21, and yyy is 1-65,535. Indicates the particular variable to be sampled. The valid variables are:

.1.3.6.1.2.1.2.2.1.10.xxx ;V InOctets: The total number of octets received on the interface, including framing characters.

.1.3.6.1.2.1.2.2.1.11.xxx ;V InUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol.

.1.3.6.1.2.1.2.2.1.12.xxx ;V InNUcastPkts: The number of broadcast and multi-cast packets delivered to a higher-layer protocol.

.1.3.6.1.2.1.2.2.1.13.xxx ;V InDiscards: The number of inbound packets that are discarded even if the packets are normal.

.1.3.6.1.2.1.2.2.1.14.xxx ;V InErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

.1.3.6.1.2.1.2.2.1.15.xxx ;V InUnknownProtos: the number of the inbound packets that were discarded because of the unknown or un-support protocol.

.1.3.6.1.2.1.2.2.1.16.xxx ;V OutOctets: The number of octets transmitted out of the interface, including framing characters.

.1.3.6.1.2.1.2.2.1.17.xxx ;V OutUcastPkts: The number of unicast packets that request to transmit.

.1.3.6.1.2.1.2.2.1.18.xxx ;V OutNUcastPkts: The number of broadcast and multi-cast packets that request to transmit.

.1.3.6.1.2.1.2.2.1.19.xxx ;V OutDiscards: The number of outbound packets that are discarded in the event the packet is normal.

.1.3.6.1.2.1.2.2.1.20.xxx ;V OutErrors: The number of outbound packets that could not be transmitted because of errors.

.1.3.6.1.2.1.2.2.1.21.xxx ;V OutQLen: The length of the output packet queue (in packets).

"xxx" above means the interface identified by a particular value of this index is the same interface as identified by the same value of OID 'ifIndex'.

absolute : Get the sample directly.

delta : Calculate the difference between samples (default).

<rising_threshold> : Rising threshold value (-2147483648;V2147483647).

<rising_event_index> : Rising event index (1-65535).

<falling_threshold> : Falling threshold value (-2147483648;V2147483647).

<falling_event_index>: Falling event index (1-65535).

rising : Trigger alarm when the first value is larger than the rising threshold.

falling : Trigger alarm when the first value is less than the falling threshold.

Note: The Rising values must be larger than the Falling values.

both : Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).

Example: >security switch rmon alarm add 1 30 .1.3.6.1.2.1.2.2.1.14.123 -2 2 -2
>

Messages: <data_source> dosen't exit

Invalid <rising_threshold> parameter: -2

Command: Delete RMON Alarm Entry

Syntax: security switch rmon alarm delete <alarm_id>

Description: Delete an existing RMON Alarm entry. The entry index key is <alarm_id>. The parameters are:
<alarm_id>: Alarm ID (1-65535).

Example: >security switch rmon alarm delete 1
>

Messages: module_id=92, code=-8

Command: Lookup RMON Alarm Entries

Syntax: security switch rmon alarm lookup [<alarm_id>]

Description: Show RMON Alarm entries. The parameters are:
<alarm_id>: Alarm ID (1-65535).

Example: >security switch rmon event lookup

Id	Description	Type	Community	LastSent
1	A	logandtrap	public	Never
2	B	snmptrap	public	Never
3	C	log	public	Never

Number of entries: 3
>

Command: Add / Modify RMON Event Entry

Syntax: security switch rmon event add <event_id> [none|log|trap|log_trap] [<community>]
[<description>]

Description: Add or modify RMON Event entry. The entry index key is <event_id>. The parameters are:
<event_id> : Event ID (1-65535).

none : Get the sample directly.

log : Get the sample directly.

trap : Get the sample directly.

log_trap : Calculate the difference between samples (default).

<community> : Specify the community when trap is sent (the string length is 0~127) (default: public).

<description>: The string for describing this event (the string length is 0~127).
(default: null string).

Example: >security switch rmon event add 1
>

Command: Delete RMON Event Entry

Syntax: security switch rmon event delete <event_id>

Description: Delete RMON Event entry. The entry index key is <event_id>. The parameters are:
<event_id>: RMON Event ID (1-65535).

Example:

```
>security switch rmon event add 1
>security switch rmon alarm delete 1
module_id=92, code=-8
>security switch rmon event lookup
Id      Description  Type           Community      LastSent
-----  -
1       1             logandtrap    public         60d 16:21:20

Number of entries: 1
>security switch rmon event delete 1
>security switch rmon event lookup
>
```

Command: Lookup RMON Event Entries

Syntax: security switch rmon event lookup [<event_id>]

Description: Show RMON Event entries, where:
<event_id>: Event ID (1-65535).

Example 1:

```
>security switch rmon event add 1
>security switch rmon event lookup
Id      Description  Type           Community      LastSent
-----  -
1       none        public 0d         00:00:01

Number of entries: 1
```

Example 2:

```
>security switch rmon event lookup
Id      Description  Type           Community      LastSent
-----  -
1       1             logandtrap    public         20057d 05:43:

Number of entries: 1
>
```

Security Switch SNMP Group

The S3280 Security Switch SNMP commands let you add, delete or look up SNMP configuration, mode, community, traps, users, groups views and/or access.

Simple Network Management Protocol (SNMP) is part of the TCP/IP protocol for network management. SNMP allows diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices running SNMP.

The SNMP agent embedded in the S3280 is capable of version 1, 2c, or v3 support to access all management information from the device. The community strings for v1 and v2c and the USM/VACM for SNMPv3 are supported. The SNMP agent can support IPv4 and IPv6 trap destinations. It also supports the INFORM PDU for notification along with traps.

Traps are generated when a condition has been met on the SNMP agent. These conditions are defined in the Management Information Base (MIB). The administrator then defines thresholds, or limits to the conditions, that are to generate a trap. Conditions range from preset thresholds to a restart.

All of the values that SNMP reports are dynamic. The information needed to get the specified values that SNMP reports is stored in the MIB. This information includes Object IDs (OIDs), Protocol Data Units (PDUs), etc. The MIBs must be located at both the agent and the manager to work effectively.

Additional SNMP traps notes:

- The Last Gasp can be in the form of IEEE802.3 2008 Clause 57 Dying gasp event and/or an SNMP trap to NMS system.
- The Y.1731 AIS and LCK faults for fault monitoring and isolation raise SNMP traps.
- All CCM errors such as remoteCCM, RDI, MACStatus, errorCCM, crossConnect, etc. are reported in MEP status and SNMP traps are raised for errors.
- SNMP traps are generated for various Threshold events (Errored Symbol Period, Errored Frame Event, Errored Frame Period Event and Errored Frame Seconds summary events) and Non-threshold events (dying gasp and critical events).
- The Link Fault, Dying Gasp, Critical Event, and other LOAM details for transmit and receive on each port are displayed at the **Monitor > Link OAM > Statistics** menu path.
- Dying Gasp is implemented as an SNMP trap and as a LOAM event.
- Trap Primary or Secondary Power Supply: with both AC and DC connected, LED S2 is green and AC is Primary. If AC is removed, LED S2 becomes AMBER indicating that the S3280 is operating with a Secondary power supply and will send out the trap as "entConfigChange".

The Security Switch SNMP Group commands available are listed below.

>security switch snmp ?

Available Commands:

Security Switch SNMP Configuration

Security Switch SNMP Mode [enable|disable]

Security Switch SNMP Version [1|2c|3]

Security Switch SNMP Read Community [<community>]

Security Switch SNMP Write Community [<community>]

Security Switch SNMP Trap Mode [enable|disable]

Security Switch SNMP Trap Version [1|2c|3]

Security Switch SNMP Trap Community [<community>]

Security Switch SNMP Trap Destination [<ip_addr_string>]

Security Switch SNMP Trap IPv6 Destination [<ipv6_addr>]

Security Switch SNMP Trap Authentication Failure [enable|disable]

Security Switch SNMP Trap Link-up [enable|disable]

Security Switch SNMP Trap Inform Mode [enable|disable]

Security Switch SNMP Trap Inform Timeout [<timeout>]

Security Switch SNMP Trap Inform Timeout [<timeout>]

Security Switch SNMP Trap Probe Security Engine ID [enable|disable]

Security Switch SNMP Trap Security Engine ID [<engineid>]

Security Switch SNMP Trap Security Name [<security_name>]

Security Switch SNMP Engine ID [<engineid>]

Security Switch SNMP Community Add <community> [<ip_addr>] [<ip_mask>]

Security Switch SNMP Community Delete <index>

Security Switch SNMP Community Lookup [<index>]

Security Switch SNMP User Add <engineid> <user_name> [MD5|SHA] [<auth_password>] [DES]
[<priv_password>]

Security Switch SNMP User Delete <index>

Security Switch SNMP User Changekey <engineid> <user_name> <auth_password> [<priv_password>]

Security Switch SNMP User Lookup [<index>]

Security Switch SNMP Group Add <security_model> <security_name> <group_name>

Security Switch SNMP Group Delete <index>

Security Switch SNMP Group Lookup [<index>]

Security Switch SNMP View Add <view_name> [included|excluded] <oid_subtree>

Security Switch SNMP View Delete <index>

Security Switch SNMP View Lookup [<index>]

Security Switch SNMP Access Add <group_name> <security_model> <security_level>
[<read_view_name>] [<write_view_name>]

Security Switch SNMP Access Delete <index>

Security Switch SNMP Access Lookup [<index>]

>

The Security Switch SNMP Group commands are explained below.

Command: Show Current SNMP Configuration
Syntax: security switch snmp configuration
Description: Show the current SNMP configuration.
Example: >security switch snmp config

```
SNMP Configuration:
=====

SNMP Mode           : Enabled
SNMP Version        : 2c
Read Community      : public
Write Community     : private
Trap Mode           : Enabled
Trap Version        : 2c
Trap Community      : public
Trap Destination    : 192.168.1.30
Trap IPv6 Destination : ::
Trap Authentication Failure : Enabled
Trap Link-up and Link-down : Enabled
Trap Inform Mode    : Enabled
Trap Inform Timeout (seconds) : 1
Trap Inform Retry Times : 5
Trap Probe Security Engine ID : Enabled
Trap Security Engine ID :
Trap Security Name  : None

SNMPv3 Engine ID : 800007e5017f000001

SNMPv3 Communities Table:
Idx Community           Source IP      Source Mask
-----
1 public                0.0.0.0      0.0.0.0
2 private               0.0.0.0      0.0.0.0

Number of entries: 2

SNMPv3 Users Table:
Idx Engine ID User Name           Level           Auth Priv
-----
1 Local      default user           NoAuth, NoPriv None None

Number of entries: 1

SNMPv3 Groups Table;
Idx Model Security Name           Group Name
-----
1 v1 public                       default ro group
2 v1 private                       default rw group
3 v2c public                       default ro group
4 v2c private                       default_rw_group
5 usm default_user                 default_rw_group

Number of entries: 5

SNMPv3 Views Table:
Idx View Name           View Type OID Subtree
-----
1 default view         included .1

Number of entries: 1

SNMPv3 Accesses Table:
Idx Group Name           Model Level
-----
1 default ro group      any NoAuth, NoPriv
2 default rw group      any NoAuth, NoPriv

Number of entries: 2
>
```

Command: **Enable or Disable SNMP Mode**
Syntax: **security switch snmp mode** [enable|disable]
Description: Set or show the SNMP mode, where:
enable : Enable SNMP.
disable: Disable SNMP.
(The default is 'Show SNMP mode'.)

```
Example: >security switch snmp mode
SNMP Mode : Enabled
>security switch snmp mode disable
>security switch snmp mode
SNMP Mode : Disabled
>security switch snmp mode enable
>security switch snmp mode
SNMP Mode : Enabled
>
```

Command: **Set or Show SNMP Version**
Syntax: **security switch snmp version** [1|2c|3]
Description: Set or show the SNMP protocol version, where:
1 : SNMP version 1.
2c: SNMP version 2c (the default setting).
3 : SNMP version 3.
(The default is 'Show SNMP version'.)

```
Example: >security switch snmp version
SNMP Version : 2c
>security switch snmp version 3
>security switch snmp version
SNMP Version : 3
>
```

Command: **Set or Show SNMP Read Community**
Syntax: **security switch snmp read community** [<community>]
Description: Set or show the community string for SNMP read access, where:
<**community**>: Community string. Use "" (double quotes) to clear the string. The maximum string length is 256 characters. (The default is 'Show SNMP read community'.)

```
Example: >security switch snmp read community
Read Community : public
>
```

Command: **Set or Show SNMP Write Community**
Syntax: **security switch snmp write community** [<community>]
Description: Set or show the community string for SNMP write access, where:
<**community**>: Community string. Use "" (double quotes) to clear the string. The maximum string length is 256 characters. (The default is 'Show SNMP write community'.)

```
Example: >security switch snmp write community
Write Community : private
>
```

Command: **Set or Show SNMP Trap Mode**
Syntax: **security switch snmp trap mode** [enable|disable]
Description: Set or show the SNMP trap mode, where:
enable : Enable SNMP traps.
disable: Disable SNMP traps.
(The default is 'Show SNMP trap mode'.)

Example:

```
>security switch snmp trap mode
Trap Mode                : Disabled
>security switch snmp trap mode enable
>security switch snmp trap mode
Trap Mode                : Enabled
>
```

Command: **Set or Show SNMP Trap Version**
Syntax: **security switch snmp trap version** [1|2c|3]
Description: Set or show the SNMP trap protocol version, where:
1 : SNMP version 1 (SNMPv1 is the initial implementation of the SNMP protocol).
2c: SNMP version 2c. SNMPv2c comprises SNMPv2 without the SNMP v2 security model, using instead the simple community-based security scheme of SNMPv1.
3 : SNMP version 3. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.
(The default is 'Show SNMP trap version'.)

Example:

```
>security switch snmp trap version
Trap Version             : 1
>security switch snmp trap version 2x
Invalid parameter: 2x

Syntax:
Security Switch SNMP Trap Version [1|2c|3]
>security switch snmp trap version 2c
>security switch snmp trap version
Trap Version             : 2c
>
```

Command: **Security Switch SNMP Trap Community**
Syntax: **security switch snmp trap community** [<community>]
Description: Set or show the community string for SNMP traps, where:
<**community**>: Community string. Use 'clear' or "" to clear the string. The maximum string length is 256 characters. (default: Show SNMP trap community)

Example:

```
>security switch snmp trap community
Trap Community           : public
>
```

Command: **Set or Show SNMP Trap Destination**
Syntax: **security switch snmp trap destination** [<ip_addr_string>]
Description: Set or show the SNMP trap destination address, where:
<**ip_addr_string**>: IP host address (a.b.c.d)

Example:

```
>security switch snmp trap community 192.168.1.30
>security switch snmp trap destination
Trap Destination        :
>
```

Command: Set or Show SNMP Trap IPv6 Destination**Syntax:** **security switch snmp trap ipv6 destination** [<ipv6_addr>]**Description:** Set or show the SNMP trap destination IPv6 address, where:
<ipv6_addr>: IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon to separate each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legal IPv4 address (e.g., '::192.1.2.34').**Example:**
>**security switch snmp trap ipv6 destination fe80::215:c5ff:fe03:4dc7**
>**security switch snmp trap ipv6 destination**
Trap IPv6 Destination : fe80::215:c5ff:fe03:4dc7
>**Command: Set or Show SNMP Trap Authentication Failure****Syntax:** **security switch snmp trap authentication failure** [enable|disable]**Description:** Set or show the SNMP authentication failure trap mode, where:
enable : Enable SNMP trap authentication failure.
disable: Disable SNMP trap authentication failure.

(The default is 'Show SNMP trap authentication failure mode'.)

Example:
>**security switch snmp trap authentication failure**
Trap Authentication Failure : Enabled
>**security switch snmp trap authentication failure disable**
>**security switch snmp trap authentication failure**
Trap Authentication Failure : Disabled
>**Command: Set or Show SNMP Trap Link-up****Syntax:** **security switch snmp trap link-up** [enable|disable]**Description:** Set or show the port link-up and link-down trap mode, where:
enable : Enable SNMP trap link-up and link-down.
disable: Disable SNMP trap link-up and link-down.

(The default is 'Show SNMP trap link-up and link-down mode'.)

Example:
>**security switch snmp trap link-up**
Trap Link-up and Link-down : Enabled
>**security switch snmp trap link-up disable**
>**security switch snmp trap link-up**
Trap Link-up and Link-down : Disabled
>**security switch snmp trap link-up enable**
>**security switch snmp trap link-up**
Trap Link-up and Link-down : Enabled
>

Command: **Set or Show SNMP Trap Inform Mode**
Syntax: **security switch snmp trap inform mode** [enable|disable]
Description: Set or show the SNMP trap inform mode, where:
enable : Enable SNMP trap inform
disable: Disable SNMP trap inform
(The default is 'Show SNMP inform mode'.)

Example:

```
>security switch snmp trap inform mode
Trap Inform Mode           : Enabled
>security switch snmp trap inform mode disable
>security switch snmp trap inform mode enable
>security switch snmp trap inform mode
Trap Inform Mode           : Enabled
>
```

Command: **Set or Show SNMP Trap Inform Timeout**
Syntax: **security switch snmp trap inform timeout** [<timeout>]
Description: Set or show the SNMP trap inform timeout (usecs), where:
<**timeout**>: SNMP trap inform timeout (0-2147 seconds).
(The default is 'Show SNMP trap inform timeout'.)

Example:

```
>security switch snmp trap inform timeout 300
>security switch snmp trap inform timeout
Trap Inform Timeout (seconds) : 300
>
```

Command: **Set or Show SNMP Trap Inform Retry Times**
Syntax: **security switch snmp trap inform retry times** [<retries>]
Description: Set or show the SNMP trap inform retry times, where:
<**retries**>: SNMP trap inform retransmitted times (0-255).
(The default is 'Show SNMP trap inform retry times'.)

Example:

```
>security switch snmp trap inform retry times 25
>security switch snmp trap inform retry times
Trap Inform Retry Times     : 25
>
```

Command: **Set or Show SNMP Trap Probe Security Engine ID**
Syntax: **security switch snmp trap probe security engine id** [enable|disable]
Description: Set or show SNMP trap security engine ID probe mode. Note that you must disable the trap security engine ID probe (using this command) before entering the **security switch snmp trap security engine id** command. The parameters are:
enable : Enable SNMP trap security engine ID probe.
disable: Disable SNMP trap security engine ID probe.
(The default is 'Show SNMP trap security engine ID probe mode'.)

Example:

```
>security switch snmp trap probe security engine id
Trap Probe Security Engine ID : Enabled
>security switch snmp trap probe security engine id disable
>security switch snmp trap probe security engine id
Trap Probe Security Engine ID : Disabled
>
```

Command: Set or Show SNMP Trap Security Engine ID

Syntax: security switch snmp trap security engine id [<engineid>]

Description: Set or show SNMP trap security engine ID. Note that you must disable the trap security engine ID probe before using this command.

The parameters are:

<engineid>: Engine ID; the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string.

Example:

```
>security switch snmp trap security engine id
Trap Security Engine ID      :
>security switch snmp trap security engine id 80 00 03 64 03 00 c0 f2 00 01 02
The format of 'Engine ID' may not be all zeros or all 'ff'H and is restricted to 5
- 32 octet string
Invalid parameter: 80
```

Syntax:

Security Switch SNMP Trap Security Engine ID [<engineid>]

```
>security switch snmp trap security engine id
```

```
Trap Security Engine ID      :
```

```
>
```

Command: Set or Show SNMP Trap Security Name

Syntax: security switch snmp trap security name [<security_name>]

Description: Set or show SNMP trap security name, where:

<security_name>: A string representing the security name for a principal. (The default is 'Show SNMP trap security name.') The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126.

Example:

```
>security switch snmp trap security name
Trap Security Name          : None
>security switch snmp trap security name moniker
Trap security engine ID should not NULL
>security switch snmp trap security name moniker827
Trap security engine ID should not NULL
>
```

Command: Set or Show SNMP Engine ID

Syntax: security switch snmp engine id [<engineid>]

Description: Set or show SNMPv3 local engine ID, where:

<engineid>: Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string.

Example:

```
>security switch snmp engine id
SNMPv3 Engine ID : 800007e5017f000001
>
```

Command: Add SNMP Community Entry**Syntax:** `security switch snmp community add <community> [<ip_addr>] [<ip_mask>]`**Description:** Add a new or modify an existing SNMPv3 community entry. The entry index key is <community>, where:

<community>: Community string.

<ip_addr> : IP address (a.b.c.d), default: Show IP address.

<ip_mask> : IP subnet mask (a.b.c.d); default: Show IP mask.

Example:
>`security switch snmp community add 192.168.1.30 255.255.255.0`
>**Command: Delete SNMP Community Entry****Syntax:** `security switch snmp community delete <index>`**Description:** Delete an existing SNMPv3 community entry, where:

<index>: entry index (1-64).

Example:
>`security switch snmp community delete 1`
>**Command: Lookup SNMP Community Entry****Syntax:** `security switch snmp community lookup [<index>]`**Description:** Lookup SNMPv3 community entry, where:

<index>: entry index (1-64).

Example:
>`security switch snmp community lookup`

Idx	Community	Source IP	Source Mask
2	private	0.0.0.0	0.0.0.0
3	192.168.1.30	0.0.0.0	0.0.0.0
4	viewonly	192.168.1.30	255.255.255.0

Number of entries: 3

>

Command: Add SNMP User

Syntax: **security switch snmp user add** <engineid> <user_name> [MD5|SHA]
 <auth_password>] [DES] [<priv_password>]

Description: Add a new SNMPv3 user entry. The entry index key are <engineid> and <user_name> and it doesn't allow modifying. The parameters are:

- <engineid>** : Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string (e.g., 800007e5017f000001).
- <user_name>** : A string identifying the user name that this entry should belong to. The name of "None" is reserved. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126.
- md5** : An optional flag to indicate that this user using MD5 authentication protocol. The allowed length is (8-32), and the allowed content is ASCII characters from 33 to 126.
- sha** : An optional flag to indicate that this user using SHA authentication protocol. The allowed length is (8-40), and the allowed content is ASCII characters from 33 to 126.
- <auth_password>**: A string identifying the authentication pass phrase.
- des** : An optional flag to indicate that this user using DES privacy protocol privacy protocol should belong to. The allowed string length is (8-32), and the allowed content is ASCII characters from 33 to 126.
- <priv_password>**: A string identifying the privacy pass phrase. The allowed string length is (8-40), and the allowed content is ASCII characters from 33 to 126.

Example:

```
>security switch snmp user add 800007e5017f000001 JeffS md5 Buffrey1 des Buffrey1
>
```

Messages:

Invalid <engineid> parameter: 123456789

Invalid parameter: sha

The format of 'Engine ID' may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string

The length is restricted to 8 - 40

The length is restricted to 8 - 40

Command: Delete SNMP User

Syntax: security switch snmp user delete <index>

Description: Delete an existing SNMPv3 user entry, where:
<index>: entry index (1-64).

Example:

```
>security switch snmp user lookup
Idx Engine ID User Name                               Level           Auth Priv
-----
1   Local      default_user   NoAuth, NoPriv None None
2   Local      JeffS          Auth, Priv     MD5  DES

Number of entries: 2
>security switch snmp user delete 2
>security switch snmp user lookup
Idx Engine ID User Name                               Level           Auth Priv
-----
1   Local      default_user   NoAuth, NoPriv None None

Number of entries: 1
>
```

Command: Change SNMP User Changekey

Syntax: security switch snmp user changekey <engineid> <user_name> <auth_password>
[<priv_password>]

Description: Change an existing SNMPv3 user's password, where:

- <engineid> : Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string.
- <user_name> : A string identifying the user name that this entry should belong to. The name of "None" is reserved. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126.
- <auth_password>: A string identifying the authentication pass phrase.
- <priv_password>: A string identifying the privacy pass phrase. The allowed string length is (8-40), and the allowed content is ASCII characters from 33 to 126.

Example:

```
>security switch snmp user changekey 800007e5017f000001 JeffS Duffrey1 Duffrey1
>
```

Messages: The entry '800007e5017f000001, JeffS' is not exist

Command: **Lookup SNMP User**
Syntax: **security switch snmp user lookup** [<index>]
Description: Lookup an existing SNMPv3 user entry, where:
 <index>: entry index (1-64).

Example:

```
>security switch snmp user lookup
>
>security switch snmp user lookup 1
Non-existing entry
>security switch snmp user lookup
Idx Engine ID User Name                               Level           Auth Priv
-----
1   Local      default_user                                         NoAuth, NoPriv None None
2   Local      JeffS                                                Auth, Priv     MD5  DES

Number of entries: 2
>
```

Command: **Add SNMP Group**
Syntax: **security switch snmp group add** <security_model> <security_name> <group_name>
Description: Add a new or modify an existing SNMPv3 group entry. The entry index keys are
 <security_model> and <security_name>. The parameters are:
 <security_model>:
 v1 - Reserved for SNMPv1.
 v2c - Reserved for SNMPv2c.
 usm - User-based Security Model (USM).
 <security_name> : A string identifying the security name that this entry should belong to.
 The allowed string length is (1-32), and the allowed content is ASCII characters
 from 33 to 126.
 <group_name> : A string identifying the group name that this entry should belong to.
 The allowed string length is (1-32), and the allowed content is ASCII characters
 from 33 to 126.

Example: >security switch snmp group add usm secgr11 gr11
 The security name '800007e5017f000001, secgr11' is not exist
 >

Command: **Delete SNMP Group**
Syntax: **security switch snmp group delete** <index>
Description: Delete an existing SNMPv3 group entry, where:
 <index>: entry index (1-64).

Example: >security switch snmp group delete 1
 >security switch snmp group delete 1
 Non-existing entry
 >

Command: **Lookup SNMP Group**

Syntax: **security switch snmp group lookup** [<index>]

Description: Lookup an existing SNMPv3 group entry, where:
 <index>: entry index (1-64)

Example:

```
>security switch snmp user lookup
```

Idx	Engine	ID	User Name	Level	Auth	Priv
1	Local		default_user	NoAuth, NoPriv	None	None
2	Local		JeffS	Auth, Priv	MD5	DES

Number of entries: 2

```
>security switch snmp group lookup
```

Idx	Model	Security Name	Group Name
1	v1	public	default_ro_group
2	v1	private	default_rw_group
3	v2c	public	default_ro_group
4	v2c	private	default_rw_group
5	usm	default_user	default_rw_group

Number of entries: 5

```
>
```

Messages: *Non-existing entry*

Command: **Add SNMP View**

Syntax: **security switch snmp view add** <view_name> [included|excluded] <oid_subtree>

Description: Add or modify SNMPv3 view entry. The entry index key are <view_name> and <oid_subtree>. The parameters are:

<view_name> : A string identifying the view name that this entry should belong to.
 The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126.

included : An optional flag to indicate that this view subtree should be included.

excluded : An optional flag to indicate that this view subtree should be excluded.

<oid_subtree>: The OID defining the root of the subtree to add to the named view.

Example:

```
>security switch snmp view add view1 included .1
```

```
>security switch snmp view lookup
```

Idx	View Name	View Type	OID Subtree
1	default_view	included	.1
2	view1	included	.1

Number of entries: 2

```
>
```

Messages: *Invalid <oid_subtree> parameter: 2345*

Command: **Delete SNMP View**

Syntax: **security switch snmp view delete** <index>

Description: Delete an existing SNMPv3 view entry, where:
 <index>: entry index (1-64).

Example:

```
>security switch snmp view delete 1
```

```
>
```

Command: **Lookup SNMP View**

Syntax: **security switch snmp view lookup** [<index>]

Description: Lookup an existing SNMPv3 view entry, where:
 <index>: entry index (1-64).

Example:

```
>security switch snmp view lookup 1
Non-existing entry
>security switch snmp view lookup
Idx View Name                               View Type  OID Subtree
-----
1   default_view                            included   .1

Number of entries: 1
>
```

Command: **Add or Change SNMP Access**

Syntax: **security switch snmp access add** <group_name> <security_model> <security_level>
 [<read_view_name>] [<write_view_name>]

Description: Add or modify SNMPv3 access entry. The entry index key are <group_name>, <security_model> and <security_level>. The parameters are:

- <group_name> : A string identifying the group name that this entry should belong to. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126.
- <security_model> : The desired SNMP model:
 - any - Accept any security model (v1|v2c|usm).
 - v1 - Reserved for SNMPv1.
 - v2c - Reserved for SNMPv2c.
 - usm - User-based Security Model (USM).
- <security_level> : noAuthNoPriv - None authentication and none privacy.
 AuthNoPriv - Authentication and none privacy.
 AuthPriv - Authentication and privacy.
- <read_view_name> : The name of the MIB view defining the MIB objects for which this request may request the current values. The name of "None" is reserved. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126.
- <write_view_name>: The name of the MIB view defining the MIB objects for which this request may potentially SET new values. The name of "None" is reserved. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126.

Example:

```
>security switch snmp access add grp1 usm AuthPriv read write
>security switch snmp access add default_ro_group usm AuthPriv read write
>
```

Messages: *The group name 'grp1' is not exist*

Note: use the ‘**security switch snmp group lookup**’ command to view / verify the addition or change.

Command: Delete SNMP Access
Syntax: `security switch snmp access delete <index>`
Description: Delete an existing SNMPv3 access entry, where:
 <index>: entry index (1-64)

Example:

```
>security switch snmp access delete 1
>security switch snmp access delete 2
>security switch snmp access delete 1
Non-existing entry
>
```

Command: Lookup SNMP Access
Syntax: `security switch snmp access lookup [<index>]`
Description: Lookup an existing SNMPv3 access entry, where:
 <index>: entry index (1-64).

Example:

```
>security switch snmp access lookup 2
Non-existing entry
>security switch snmp access lookup 1
Entry Index      : 1
Group Name       : default_ro_group
Security Model    : any
Security Level   : NoAuth, NoPriv
Read View Name   : default_view
Write View Name  : None
>security switch snmp access lookup
```

Idx	Group Name	Model	Level
1	default_ro_group	any	NoAuth, NoPriv
2	default_rw_group	any	NoAuth, NoPriv
3	default_ro_group	usm	Auth, Priv

```
Number of entries: 3
>
```

Security > Network Commands

The S3280 supports these security network command sub-groups:

>security network ?

Command Groups:

```
-----
Security Network Psec : Port Security Status
Security Network Limit : Port Security Limit Control
Security Network NAS : Network Access Server (IEEE 802.1X)
Security Network ACL : Access Control List
Security Network DHCP : Dynamic Host Configuration Protocol
Security Network IP : IP Source Guard
Security Network ARP : Address Resolution Protocol
```

The S3280 security network sub-group commands are explained below.

Security Network Psec Group

The security network Psec (port security) commands are explained below.

Command: Show Current Port Security Status

Syntax: security network psec switch [<port_list>]

Description: Show the current Port Security status, where:
<port_list>: Port list or 'All'. The default is 'All. ports.

```
Example: >security network psec switch
Users:
L = Limit Control
8 = 802.1X
D = DHCP Snooping

Port  Users  State          MAC Cnt
-----  -----  -----
1     ---    No users      0
2     ---    No users      0
3     ---    No users      0
4     ---    No users      0
5     -8-    Ready         0
6     ---    No users      0
7     ---    No users      0
8     ---    No users      0
>
```

Command: Show Port Security Addresses

Syntax: security network psec port [<port_list>]

Description: Show the MAC Addresses learned by Port Security, where:
<port_list>: Port list or 'All'. The default is 'All' ports.

Example:

```
>security network psec port 1,2

Port 1:
-----
MAC Address          VID    State      Added                                     Age/Hold Time
-----
<none>

Port 2:
-----
MAC Address          VID    State      Added                                     Age/Hold Time
-----
<none>
```

Security Network Limit Group

Command: Show Current Limit Configuration

Syntax: security network limit config [<port_list>]

Description: Show the existing Limit Control configuration, where:
<port_list>: Port list or 'All'. The default is 'All' ports.

Example:

```
>security network limit config

Port Security Limit Control Configuration:
=====

Mode       : Disabled
Aging      : Disabled
Age Period: 3600

Port  Mode       Limit  Action      State
-----
  1  Disabled     4     None        Disabled
  2  Disabled     4     None        Disabled
  3  Disabled     4     None        Disabled
  4  Disabled     4     None        Disabled
  5  Disabled     4     None        Disabled
  6  Disabled     4     None        Disabled
  7  Disabled     4     None        Disabled
  8  Disabled     4     None        Disabled
>
```


Command: Set / Show Limit Mode

Syntax: security network limit mode [enable|disable]

Description: Set or show global enabled state, where:
enable : Globally enable port security.
disable : Globally disable port security.
 (default: Show current global enabled state of port security limit control)

Example:

```
>security network limit mode
Mode      : Enabled
>security network limit mode disable
>security network limit mode
Mode      : Disabled
>
```

Command: Set / Show MAC Address Aging

Syntax: security network limit aging [enable|disable]

Description: Set or show the MAC address aging enabled state, where:
enable : Enable aging.
disable : Disable aging.
 (default: Show the current state of aging)

Example:

```
>security network limit aging
Aging     : Enabled
>security network limit aging disable
>security network limit aging
Aging     : Disabled
>
```

Command: Set / Show MAC Address Agetime Limit

Syntax: security network limit agetime [<age_time>]

Description: Set or show the time in seconds between checks for activity on learned MAC addresses.
 The parameters are:
 <age_time>: Time in seconds between checks for activity on a MAC address. The valid range is 10-10000000 seconds). The default is 'Show current age time'.

Example:

```
>security network limit agetime
Age Period: 360
>security network limit agetime 600
>security network limit agetime
Age Period: 600
>
```

Command: Set / Show Limit Port Security State

Syntax: security network limit port [<port_list>] [enable|disable]

Description: Set or show the per-port enabled state, where:
<port_list>: Port list or 'all'. The default is 'All' ports.

enable : Enable port security on this port.

disable : Disable port security on this port.

(The default is 'Show current port enabled state of port security limit control'.)

Example: >security network limit port

Port	Mode	Limit	Action	State
1	Disabled	4	None	Disabled
2	Disabled	4	None	Disabled
3	Disabled	4	None	Disabled
4	Disabled	4	None	Disabled
5	Disabled	4	None	Disabled
6	Disabled	4	None	Disabled
7	Disabled	4	None	Disabled
8	Disabled	4	None	Disabled

>security network limit port 2 enable

>security network limit port

Port	Mode	Limit	Action	State
1	Disabled	4	None	Disabled
2	Enabled	4	None	Disabled
3	Disabled	4	None	Disabled
4	Disabled	4	None	Disabled
5	Disabled	4	None	Disabled
6	Disabled	4	None	Disabled
7	Disabled	4	None	Disabled
8	Disabled	4	None	Disabled

>

Command: Set / Show Learned Port Limit

Syntax: security network limit limit [<port_list>] [<limit>]

Description: Set or show the maximum number of MAC addresses that can be learned on this set of ports. The parameters are:

<port_list>: Port list or 'All'. The default is 'All' ports.

<limit> : Max. number of MAC addresses on this port.

(The default is 'Show current limit'.)

Example:

```
>security network limit limit
Port  Mode      Limit  Action  State
----  -
 1  Disabled   4  None   Disabled
 2  Disabled   4  None   Disabled
 3  Disabled   4  None   Disabled
 4  Disabled   4  None   Disabled
 5  Disabled   4  None   Disabled
 6  Disabled   4  None   Disabled
 7  Disabled   4  None   Disabled
 8  Disabled   4  None   Disabled
>security network limit limit 1,2 2
>security network limit limit
Port  Mode      Limit  Action  State
----  -
 1  Disabled   2  None   Disabled
 2  Enabled    2  None   Disabled
 3  Disabled   4  None   Disabled
 4  Disabled   4  None   Disabled
 5  Disabled   4  None   Disabled
 6  Disabled   4  None   Disabled
 7  Disabled   4  None   Disabled
 8  Disabled   4  None   Disabled
>
```

Command: Set / Show Exceeded Limit Action

Syntax: security network limit action [<port_list>] [none|trap|shut|trap_shut]

Description: Set or show the action involved with exceeding the limit, where:

<port_list> : Port list or 'all', default: All ports

none|trap|shut|trap_shut: Action to take if the number of MAC addresses exceeds the limit.

none : Don't do anything.

trap : Send an SNMP trap.

shut : Shutdown the port.

trap_shut: Send an SNMP trap and shutdown the port.

(The default is 'Show current action'.)

Example:

```
>security network limit action

Port  Mode      Limit  Action          State
-----
  1  Disabled    2     None            Disabled
  2  Enabled     2     None            Disabled
  3  Disabled    4     None            Disabled
  4  Disabled    4     None            Disabled
  5  Disabled    4     None            Disabled
  6  Disabled    4     None            Disabled
  7  Disabled    4     None            Disabled
  8  Disabled    4     None            Disabled

>security network limit action 1,3 trap_shut
>security network limit action

Port  Mode      Limit  Action          State
-----
  1  Disabled    2     Trap & Shutdown Disabled
  2  Enabled     2     None            Disabled
  3  Disabled    4     Trap & Shutdown Disabled
  4  Disabled    4     None            Disabled
  5  Disabled    4     None            Disabled
  6  Disabled    4     None            Disabled
  7  Disabled    4     None            Disabled
  8  Disabled    4     None            Disabled

>
```

Command: Reopen Port with Limit Exceeded

Syntax: security network limit reopen [<port_list>]

Description: Reopen one or more ports whose limit is exceeded and shut down. The parameters are:

<port_list>: Port list or 'All'. The default is 'All' ports.

Example:

```
>security network limit reopen
>
```

Security Network NAS Group

These commands let you configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the ‘backend’ servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured with the AAA menu commands. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as explained below.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. A device uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

IEEE 802.1X Port-based Network Access Control provides a standard for authenticating and authorizing devices attached to a LAN port. Generally, IEEE 802.1X is port-based; however, the S3280 also supports MAC-based network access control.

The NAS configuration consists of system-level and port-level NAS configuration.

The available Security Network NAS group commands are listed below.

>security network nas ?

Available Commands:

```

Security Network NAS Configuration [<port_list>]
Security Network NAS Mode [enable|disable]
Security Network NAS State [<port_list>] [auto|authorized|unauthorized|single|multi|macbased]
Security Network NAS Reauthentication [enable|disable]
Security Network NAS ReauthPeriod [<reauth_period>]
Security Network NAS EapolTimeout [<eapol_timeout>]
Security Network NAS Agetime [<age_time>]
Security Network NAS Holdtime [<hold_time>]
Security Network NAS RADIUS_QoS [global|<port_list>] [enable|disable]
Security Network NAS RADIUS_VLAN [global|<port_list>] [enable|disable]
Security Network NAS Guest_VLAN [global|<port_list>] [enable|disable] [<vid>] [<reauth_max>]
[<allow_if_eapol_seen>]
Security Network NAS Authenticate [<port_list>] [now]
Security Network NAS Statistics [<port_list>] [clear|eapol|radius]
>

```

The available Security Network NAS group commands are explained below.

Command: Show Current NAS Configuration

Syntax: security network nas configuration [<port_list>]

Description: Show 802.1X configuration, where:
 <port_list>: Port list or 'All'. The default is 'All' ports.

Example:

```
>security network nas config

802.1X Configuration:
=====
Mode                : Enabled
Reauth.             : Disabled
Reauth. Period     : 3600
EAPOL Timeout      : 30
Age Period         : 300
Hold Time          : 10
RADIUS QoS         : Enabled
RADIUS VLAN        : Enabled
Guest VLAN         : Enabled
Guest VLAN ID      : 1
Max. Reauth Count  : 2
Allow Guest VLAN if EAPOL Frame Seen: Enabled

Port  Admin State          Port State          Last Source          Last ID
-----
1     Force Authorized      Authorized          -                    -
2     Port-based 802.1X      Link Down          -                    -
3     Single 802.1X         Link Down          -                    -
4     Multi 802.1X          Link Down          -                    -
5     MAC-Based Auth        0 Auth/0 Unauth   -                    -
6     Force Authorized      Link Down          -                    -
7     Force Authorized      Link Down          -                    -
8     Force Authorized      Link Down          -                    -
>
```

Command: Set or Show Global NAS Mode

Syntax: security network nas mode [enable|disable]

Description: Set or show the global NAS state, where:
enable : Globally enable 802.1X.
disable: Globally disable 802.1X.
 (The default is 'Show current 802.1X global state'.)

Example:

```
>security network nas mode
Mode                : Disabled
>security network nas mode enable
>security network nas mode
Mode                : Enabled
>
```

Command: Set or Show NAS Security State

Syntax: security network nas state [<port_list>] [auto|authorized|unauthorized|single|multi|macbased]

Description: Set or show the port security state, where:
 <port_list>: Port list or 'All'. The default is 'All' ports.
auto : Port-based 802.1X Authentication.
authorized : Port access is allowed.
unauthorized: Port access is not allowed.
single : Single Host 802.1X Authentication.
multi : Multiple Host 802.1X Authentication.
macbased : Switch authenticates on behalf of the client.
 (The default is 'Show 802.1X state'.)

Example:

```
>security network nas state
```

Port	Admin State	Port State	Last Source	Last ID
1	Force Authorized	Authorized	-	-
2	Port-based 802.1X	Link Down	-	-
3	Single 802.1X	Link Down	-	-
4	Multi 802.1X	Link Down	-	-
5	MAC-Based Auth	0 Auth/0 Unauth	-	-
6	Force Authorized	Link Down	-	-
7	Force Authorized	Link Down	-	-
8	Force Authorized	Link Down	-	-

```
>
```

Messages: Port 9: The 802.1X Admin State must be set to Authorized for ports that are enabled for Spanning Tree

Command: Set or Show NAS Reauthentication State

Syntax: security network nas reauthentication [enable|disable]

Description: Set or show Reauthentication state, where:
enable : Enable reauthentication.
disable: Disable reauthentication.
 (The default is 'Show current reauthentication mode'.)

Example:

```
>security network nas reauthentication
Reauth.          : Disabled
>security network nas reauthentication enable
>security network nas reauthentication
Reauth.          : Enabled
>
```

Command: Set or Show NAS Reauthentication Period

Syntax: security network nas reauthperiod [<reauth_period>]

Description: Set or show the period between reauthentications. The parameters are:
<reauth_period>: The Period between reauthentications (1-3600 seconds).
(The default is 'Show current reauthentication period'.)

Example:

```
>security network nas reauthperiod
Reauth. Period   : 3600
>security network nas reauthperiod 600
>security network nas reauthperiod
Reauth. Period   : 600
>
```

Command: Set or Show NAS EAPOL Timeout

Syntax: security network nas eapoltimeout [<eapol_timeout>]

Description: Set or show the time between EAPOL retransmissions. The parameters are:
<eapol_timeout>: Time between EAPOL retransmissions (1-65535 seconds).
(The default is 'Show current EAPOL retransmission timeout'.)

Example:

```
>security network nas eapoltimeout
EAPOL Timeout    : 30
>security network nas eapoltimeout 45
>security network nas eapoltimeout
EAPOL Timeout    : 45
>
```

Command: Set or Show NAS Agetime

Syntax: security network nas agetime [<age_time>]

Description: Set or show the Time in seconds between check for activity on successfully authenticated MAC addresses. The parameters are:
<age_time>: Time between checks (10-1000000 seconds).
(The default is 'Show current age time'.)

Example:

```
>security network nas agetime
Age Period       : 300
>security network nas agetime 600
>security network nas agetime
Age Period       : 600
>
```

Command: Set or Show NAS Holdtime

Syntax: security network nas holdtime [<hold_time>]

Description: Set or show the Time in seconds before a MAC-address that failed authentication gets a new authentication chance. The parameters are:
<hold_time>: Time on hold (10-1,000,000 seconds).
(The default is 'Show current hold time'.)

Example:

```
>security network nas holdtime
Hold Time        : 10
>security network nas holdtime 60
>security network nas holdtime
Hold Time        : 60
>
```


Command: Set or Show NAS RADIUS_QoS

Syntax: security network nas radius_qos [global|<port_list>] [enable|disable]

Description: Set or show either global state (use the global keyword) or per-port state of RADIUS-assigned QoS. The default is 'show the current RADIUS-assigned QoS state'. The parameters are:

global : Select the global RADIUS-assigned QoS setting.

<port_list>: Select the per-port RADIUS-assigned QoS setting.

(The default is 'Show current per-port RADIUS-assigned QoS state'.)

enable : Enable RADIUS-assigned QoS either globally or on one or more ports.

disable: Disable RADIUS-assigned QoS either globally or on one or more ports.

Example 1:

```
>security network nas radius_qos global
RADIUS QoS      : Disabled
>security network nas radius_qos global enable
>security network nas radius_qos

      RADIUS
Port  QoS      Current
----  -
1     Disabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
>
```

Example 2:

```
>security network nas radius_qos 2,3,4 enable
>security network nas radius_qos

      RADIUS
Port  QoS      Current
----  -
1     Disabled
2     Enabled
3     Enabled
4     Enabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
>
```

Command: Set or Show NAS RADIUS_VLAN

Syntax: security network nas radius_vlan [global|<port_list>] [enable|disable]

Description: Set or show either global state (use the global keyword) or per-port state of RADIUS-assigned VLAN. The parameters are:

global : Select the global RADIUS-assigned VLAN setting.

<port_list>: Select the per-port RADIUS-assigned VLAN setting.

(The default is 'Show current per-port RADIUS-assigned VLAN state'.)

enable : Enable RADIUS-assigned VLAN either globally or on one or more ports.

disable: Disable RADIUS-assigned VLAN either globally or on one or more ports.

(The default is 'Show current RADIUS-assigned VLAN state'.)

Example:

```
>security network nas radius_vlan

      RADIUS
Port  VLAN      Current
----  -
1     Disabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
>security network nas radius_vlan 1,2,3

      RADIUS
Port  VLAN      Current
----  -
1     Disabled
2     Disabled
3     Disabled
>security network nas radius_vlan 1,2,3 enable
>security network nas radius_vlan 1,2,3,4

      RADIUS
Port  VLAN      Current
----  -
1     Enabled
2     Enabled
3     Enabled
4     Disabled
>
```

Command: Set or Show NAS Guest_VLAN

Syntax: security network nas guest_vlan [global|<port_list>] [enable|disable] [<vid>] [<reauth_max>] [<allow_if_eapol_seen>]

Description: Set or show either global state and parameters (use the global keyword) or per-port state of the Guest VLAN. Unless the 'global' keyword is used, the <reauth_max> and <allow_if_eapol_seen> parameters will not be unused. The parameters are:

global : Select the global Guest VLAN setting.

<port_list>: Select the per-port Guest VLAN setting.
(The default is 'Show current per-port Guest VLAN state'.)

enable|disable : enable : Enable Guest VLAN either globally or on one or more ports.
disable: Disable Guest VLAN either globally or on one or more ports.
(The default is 'Show current Guest VLAN state'.)

<vid> : Guest VLAN ID used when entering the Guest VLAN. Use the 'global' keyword to change it.
(The default is 'Show current Guest VLAN ID/.')

<reauth_max> : The value can only be set if you use the 'global' keyword in the beginning of the command. This is the number of times a Request Identity EAPOL frame is sent without response before considering entering the Guest VLAN.
(The default is 'Show current Maximum Reauth Count value'.)

<allow_if_eapol_seen>: The value can only be set if you use the 'global' keyword in the beginning of the command.
disable:The Guest VLAN can only be entered if no EAPOL frames have been received on a port for the lifetime of the port.
enable :The Guest VLAN can be entered even if an EAPOL frame has been received during the lifetime of the port.
(The default is 'Show current setting'.)

Example:

```
>security network nas guest_vlan

      Guest
Port  VLAN      Current
----  -
1     Disabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled

>security network nas guest_vlan 1 enable
>security network nas guest_vlan

      Guest
Port  VLAN      Current
----  -
1     Enabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled

>
```

Command: Restart NAS Authentication Process**Syntax:** `security network nas authenticate [<port_list>] [now]`**Description:** Refresh (restart) the 802.1X authentication process. The parameters are:
<port_list>: Port list or 'All'. The default is 'All' ports.
now : Force reauthentication immediately.
(default: Schedule a reauthentication)**Example:**

```
>security network nas authenticate 8
>
```

Command: Show / Clear NAS Statistics**Syntax:** `security network nas statistics [<port_list>] [clear|eapol|radius]`**Description:** Show or clear 802.1X statistics, where:
<port_list>: Port list or 'All'. The default is 'All' ports.
clear : Clear statistics.
eapol : Show EAPOL statistics.
radius : Show Backend Server statistics.**Example:**

```
>security network nas statistics 1

Port 1 EAPOL Statistics:

Rx Total:                0      Tx Total:                0
Rx Response/Id:         0      Tx Request/Id:         0
Rx Response:            0      Tx Request:            0
Rx Start:               0
Rx Logoff:              0
Rx Invalid Type:        0
Rx Invalid Length:      0

Port 1 Backend Server Statistics:

Rx Access Challenges:    0      Tx Responses:          0
Rx Other Requests:      0
Rx Auth. Successes:     0
Rx Auth. Failures:      0
>
```

Security Network ACL Group

These commands let you configure the ACL parameters (ACE) of each S3280 port. The parameters will affect frames received on a port unless the frame matches a specific ACE. Each ACE (Access Control Entry) describes the access permission associated with a particular ACE ID.

Using ACLs (Access Controls Lists), the S3280 can ‘peek’ into the frames at line rate and is capable of deep packet inspection; this ability gives a whole range of access controls. The rules or the access control lists can look at any field in the Layer 2 to Layer 4 headers to make the decision to allow / discard / mirror / log or even shutdown the port that the frame came through.

The ACL rule created can be associated with any port as well when created as a policy. Apart from the ACL, there is a device level option to do storm prevention for the unicast, multicast and broadcast frames.

The reserved ACEs used for internal protocol cannot be edited or deleted, the order sequence cannot be changed, and the priority is highest. Each ACE describes access permissions associated with a particular ACE ID. There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, varied parameter options that are available for individual application. An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected. A frame that hits this ACE matches the configuration that is defined here.

The available Security Network ACL (Access Control List) group commands are listed below.

>security network acl ?

Available Commands:

Security Network ACL Configuration [<port_list>]

Security Network ACL Action [<port_list>] [permit|deny] [<rate_limiter>] [<evc_policer>] [<port_redirect>] [<mirror>] [<logging>] [<shutdown>]

Security Network ACL Policy [<port_list>] [<policy>]

Security Network ACL Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]

Security Network ACL Add [<ace_id>] [<ace_id_next>]

[(port <port_list>)] [(policy <policy> <policy_bitmask>)]

[<tagged>] [<vid>] [<tag_prio>] [<dmac_type>]

[(etype [<etype>] [<smac>] [<dmac>]) |

(arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>)] |

(ip [<sip>] [<dip>] [<protocol>] [<ip_flags>)] |

(icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>)] |

(udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>)] |

(tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>)] |

[permit|deny] [<rate_limiter>] [<evc_policer>] [<port_redirect>] [<mirror>] [<logging>] [<shutdown>]

Security Network ACL Delete <ace_id>

Security Network ACL Lookup [<ace_id>]

Security Network ACL Clear

Security Network ACL Status [combined|static|link_oam|dhcp|ptp|arp_inspection|mep|ipmc|ip_source_guard|conflicts]

Security Network ACL Port State [<port_list>] [enable|disable]

The available Security Network ACL Group commands are explained below.

Command: Display Current ACL Configuration
Syntax: security network acl configuration [<port_list>]
Description: Show the current ACL configuration, where:
 <port_list>: Port list or 'all'. the default is 'All' ports.

Example:

```
>security network acl config

ACL Configuration:
=====

Port  Policy  Action  Rate L.  EVC P.  Port C.  Mirror  Logging  Shutdown  Counter
-----
1      0      Permit  Disabled Disabled Disabled Disabled Disabled Disabled 5376
2      0      Permit  Disabled Disabled Disabled Disabled Disabled Disabled 0
3      0      Permit  Disabled Disabled Disabled Disabled Disabled Disabled 0
4      0      Permit  Disabled Disabled Disabled Disabled Disabled Disabled 0
5      0      Permit  Disabled Disabled Disabled Disabled Disabled Disabled 0
6      0      Permit  Disabled Disabled Disabled Disabled Disabled Disabled 0
7      0      Permit  Disabled Disabled Disabled Disabled Disabled Disabled 0
8      0      Permit  Disabled Disabled Disabled Disabled Disabled Disabled 0

Rate Limiter  Rate
-----
1              1 PPS
2              1 PPS
3              1 PPS
4              1 PPS
5              1 PPS
6              1 PPS
7              1 PPS
8              1 PPS
9              1 PPS
10             1 PPS
11             1 PPS
12             1 PPS
13             1 PPS
14             1 PPS
15             1 PPS
16             1 PPS

ID  Type  Port  Policy  Frame  Action  Rate L.  Port C.  Mirror  Counter
--  ---  ---  ---    ---    ---    ---    ---    ---    ---
1   User  1-8  Any     Any     Permit  Disabled Disabled Disabled 999

Number of ACEs: 1
>
```

Note: This command uses these abbreviations:

- Rate L.** = Rate Limiter
- EVC P.** = EVC Policer
- Port C.** = Port Copy (redirect)

Command: Set / Show ACL Port Default Action

Syntax: **security network acl action** [<port_list>] [permit|deny] [<rate_limiter>]
 [<evc_policer>] [<port_redirect>] [<mirror>] [<logging>] [<shutdown>]

Description: Set or show the ACL port default action. Note that an ACL policer and an EVC policer can not both be enabled at the same time. The parameters are:

<port_list> : Port list or 'all', default: All ports.
 permit : Permit forwarding (default).
 deny : Deny forwarding.
 <rate_limiter>: Rate limiter number (1-15) or 'disable'.
 <evc_policer> : EVC policer number (1-128) or 'disable'.
 <port_redirect>: Port list for copy of frames or 'disable'
 <mirror> : Mirror of frames: enable|disable.
 <logging> : System logging of frames: log|log_disable.
 <shutdown> : Shut down ingress port: shut|shut_disable.

Example:

```
>security network acl action
```

Port	Action	Rate L.	EVC P.	Port C.	Mirror	Logging	Shutdown	Counter
1	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	5378
2	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0
3	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0
4	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0
5	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0
6	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0
7	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0
8	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0

```
>security network acl action 1,2,3 deny 5 7 5 enable log shut
```

```
>security network acl action 1,2,3 deny 5 disable 6,7 enable log shut
```

```
>
```

Messages:

```
>security network acl action 1,2,3 deny 5 7 5 enable log shut
```

```
>E api/cil 03:44:05 31/126_action_check#5964: Error: ACL policer and EVC policer  

  can not both be enabled
```

```
>security network acl action 1,2,3 deny 5 disable 6,7 enable log shut
```

```
>E api/cil 03:46:32 31/126_acl_policer_free#5997: Error: policer 0 already free
```

```
>security network acl action 1,2,3 deny 5 disable 6,7 enable log shut
```

```
>
```

The 'show' version of the command uses these abbreviations:

Rate L. = Rate Limiter

EVC P. = EVC Policer

Port C. = Port Copy (redirect)

Command: Set / Show ACL Port Policy

Syntax: security network acl policy [<port_list>] [<policy>]

Description: Set or show the current ACL port policy, where:
<port_list>: Port list or 'All'. The default is 'All ports'.
<policy> : Policy number (0-255).

Example:

```
>security network acl policy

Port  Policy
----  -
1     0
2     0
3     0
4     0
5     0
6     0
7     0
8     0

>security network acl policy 1 2
>security network acl policy 4 26
>security network acl policy

Port  Policy
----  -
1     2
2     0
3     0
4     26
5     0
6     0
7     0
8     0
>
```

Messages:

E api/cil 03:02:07 28/126_acl_policer_free#5517: Error: policer 0 already free

Command: Set / Show ACL Rate

Syntax: security network acl rate [<rate_limiter_list>] [<rate_unit>] [<rate>]

Description: Set or show the ACL rate limiter, where:

<rate_limiter_list>: Rate limiter list (1-16). The default is All rate limiters.

<rate_unit> : IP flags: pps|kbps, default: pps (packets per second).

<rate> : Rate in pps (0-100) or kbps (0, 100, 2*100, 3*100, ..., 1000000 bits per second).

Example:

```
>security network acl rate 1,2 kbps 100
>security network acl rate
```

```
Rate Limiter  Rate
-----
1             100 KBPS
2             100 KBPS
3             1 PPS
4             1 PPS
5             1 PPS
6             1 PPS
7             1 PPS
8             1 PPS
9             1 PPS
10            1 PPS
11            1 PPS
12            1 PPS
13            1 PPS
14            1 PPS
15            1 PPS
16            1 PPS
>
```

Messages: Invalid parameter: 3*100

Command: Add / Modify ACE

Syntax: Security Network ACL Add [<ace_id>] [<ace_id_next>]
 (port <port_list>)] [(policy <policy> <policy_bitmask>)]
 [<tagged>] [<vid>] [<tag_prio>] [<dmac_type>]
 [(etype [<etype>] [<smac>] [<dmac>])] |
 (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) |
 (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) |
 (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) |
 (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) |
 (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])]
 [permit|deny] [<rate_limiter>] [<evc_policer>] [<port_redirect>] [<mirror>] [<logging>]
 [<shutdown>]

Description: Add a new or modify an existing Access Control Entry (ACE).

If the ACE ID parameter <ace_id> is specified and an entry with this ACE ID already exists, the ACE will be modified. Otherwise, a new ACE will be added.

If the ACE ID is not specified, the next available ACE ID will be used.

If the next ACE ID parameter <ace_id_next> is specified, the ACE is placed before this ACE in the list.

If the next ACE ID is not specified, the ACE will be placed last in the list.

If the Switch keyword is used, the rule applies to all ports.

If the Port keyword is used, the rule applies to the specified port only.

If the Policy keyword is used, the rule applies to all ports configured with the specified policy.

The default is that the rule applies to all ports.

The parameters are:

<ace_id> : ACE ID (1-256). The default is the next available ACE ID.

<ace_id_next> : Next ACE ID (1-256). The default is 'Add ACE last'.

port : Port ACE keyword.

<port_list> : Port list or 'All'. The default is 'All' ports.

policy : Policy ACE keyword.

<policy> : Policy number (0-255).

<policy_bitmask>: Policy number bitmask (0x0 - 0xFF).

<tagged> : Tagging of frames (any / enable / disable).

<vid> : VLAN ID (1-4094) or 'Any'.

<tag_prio> : VLAN tag priority (0-7) or 'Any'.

<dmac_type> : DMAC type (any / unicast / multicast / broadcast).

etype : Ethernet Type keyword.

<etype> : Ethernet Type: 0x600 - 0xFFFF or 'any' but excluding 0x800(IPv4) 0x806(ARP) and 0x86DD(IPv6).

<smac> : Source MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', where x is a hexadecimal digit) or 'Any'.

<dmac> : Destination MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', where x is a hexadecimal digit) or 'Any'.

arp : ARP keyword.

<sip> : Source IP address (a.b.c.d/n) or 'Any'.

<dip> : Destination IP address (a.b.c.d/n) or 'Any'.

<arp_opcode> : ARP operation code (any / arp / rarp / other).

<arp_flags> : ARP flags (request / smac / dmac / len / ip / ether [0|1|any]).
ip : IP keyword
<protocol> : IP protocol number (0-255) or 'Any'.
<ip_flags> : IP flags: ttl / options / fragment [0|1|any].
icmp : ICMP keyword.
<icmp_type> : ICMP type number (0-255) or 'Any'.
<icmp_code> : ICMP code number (0-255) or 'Any'.
udp : UDP keyword.
<sport> : Source UDP/TCP port range (0-65535) or 'Any'.
<dport> : Destination UDP/TCP port range (0-65535) or 'Any'.
tcp : TCP keyword.
<tcp_flags> : TCP flags: fin / syn / rst / psh / ack / urg [0|1|any].
permit : Permit forwarding (default).
deny : Deny forwarding.
<rate_limiter> : Rate limiter number (1-15) or 'disable'.
<evc_policer> : EVC policer number (1-128) or 'disable'.
<port_redirect> : Port list for copy of frames or 'disable'.
<mirror> : Mirror of frames: enable / disable.
<logging> : System logging of frames: log / log_disable.
<shutdown> : Shut down ingress port: shut / shut_disable.

Example:

```

>security network acl add 1 2 3 4 5 6 7 8 9
>security network acl add
ACE ID 1 added last
>

```

Messages:

ACL Add failed

Invalid parameter: 8

Command: **Delete Existing ACL Entry**

Syntax: **security network acl delete <ace_id>**

Description: Deletes (removes) an existing ACL entry from the table, where:

<ace_id>: ACE ID (1-256)

Example:

```

>security network acl delete 1
ACL Delete failed
>security network acl delete 0
Invalid <ace_id> parameter: 0

```

Command: **Lookup ACL ACE(s)**

Syntax: **security network acl lookup** [<ace_id>]

Description: Show all or specified existing ACE(s). Default: All ACEs. The parameters are:
<ace_id>: ACE ID (1-256).

Example:

```
>security network acl lookup
ID   Type      Port      Policy      Frame      Action Rate L.  Port C.  Mirror  Counter
---  -
1    User      1-8      Any         Any        Permit Disabled Disabled Disabled 35879
```

Number of ACEs: 1

>

```
>security network acl add
```

ACE ID 2 added last

```
>security network acl lookup
```

```
ID   Type      Port      Policy      Frame      Action Rate L.  Port C.  Mirror  Counter
---  -
1    User      1-8      Any         Any        Permit Disabled Disabled Disabled 1006
2    User      1-8      Any         Any        Permit Disabled Disabled Disabled 0
```

Number of ACEs: 2

>

Messages:

ACL Add failed

Invalid parameter: 8

Command: **Clear ACL Counters**

Syntax: **security network acl clear**

Description: Clear all ACL counters.

Example: >security network acl clear
>

Command: Show Current ACL Status

Syntax: security network acl status

[combined|static|link_oam|dhcp|ptp|arp_inspection|mep|ipmc|ip_source_guard|conflicts]

Description: Show current ACL status, where:

combined : Show combined status.

static : Show static user configured status.

link_oam : Show Link OAM status.

dhcp : Show DHCP status.

ptp : Show PTP status.

arp_inspection : Show ARP Inspection status.

mep : Show MEP status.

ipmc : Show IPMC status.

ip_source_guard : Show IP Source Guard status.

conflicts : Show conflict status.

(The default is 'Show combined status'.)

Example:

```
>security network acl status
```

```
User
```

```
----
```

```
S : Static
```

```
IPSG: IP Source Guard
```

```
IPMC: IPMC
```

```
MEP : MEP
```

```
ARPI: ARP Inspection
```

```
PTP : PTP
```

```
DHCP: DHCP
```

```
LOOP: Loop Protect
```

```
LOAM: Link OAM
```

User ID	Port	Frame	Action	Rate L.	Port C.	Mirror	CPU	Counter	Confl.
LOOP 1	1-9	EType	Deny	Disabled	Disabled	Disabled	Yes	0	No
DHCP 1	1-9	UDP	Deny	Disabled	Disabled	Disabled	Yes	0	No
DHCP 2	1-9	UDP	Deny	Disabled	Disabled	Disabled	Yes	0	No
PTP 1	2,3	EType	Deny	Disabled	Disabled	Disabled	Yes	0	No
PTP 2	2,3	EType	Deny	Disabled	Disabled	Disabled	Yes	0	No
MEP 5	2	EType	Deny	Disabled	Disabled	Disabled	No (0)	0	No
MEP 4	1	EType	Deny	Disabled	Disabled	Disabled	No (0)	0	No
MEP 1	2	EType	Deny	Disabled	Disabled	Disabled	Yes	0	No
MEP 2	1,2	EType	Deny	Disabled	Disabled	Disabled	Yes	0	No
MEP 3	1	EType	Deny	Disabled	Disabled	Disabled	No	0	No
IPSG 1	2,3	IP	Deny	Disabled	Disabled	Disabled	No	0	No
S 1	1-8	Any	Permit	Disabled	Disabled	Disabled	No	1006	No
S 2	1-8	Any	Permit	Disabled	Disabled	Disabled	No	0	No

```
Number of ACEs: 13
```

```
>
```

Command: Set / Show ACL Port State

Syntax: security network acl port state [<port_list>] [enable|disable]

Description: Set or show the ACL port state, where:

<port_list> : Port list or 'All'. The default is All ports.

enable|disable: ACL port state enable or disable.

Example: >security network acl port state 2 disable
>security network acl port state

```
Port  State
----  -
1     Disabled
2     Disabled
3     Enabled
4     Enabled
5     Enabled
6     Enabled
7     Enabled
8     Enabled
>
```

Security Network DHCP Group

DHCP (Dynamic Host Configuration Protocol) is used for assigning dynamic IP addresses to devices on a network. DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a 'bogus' DHCP reply packet to a legitimate conversation between the DHCP client and server.

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain. The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit. The definition of Circuit ID in the switch is 4 bytes long and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The "module_id" parameter is the third byte for the module ID (in standalone switch it always equal 0). The "port_no" parameter is the fourth byte and it means the port number.

The Remote ID is 6 bytes long, and the value is equal to the DHCP relay agents MAC address.

This group includes the following DHCP Relay and DHCP Snooping commands.

```
>security network dhcp ?
```

```
Available Commands:
```

Security Network DHCP Relay Configuration

```
Security Network DHCP Relay Mode [enable|disable]
```

```
Security Network DHCP Relay Server [<ip_addr>]
```

```
Security Network DHCP Relay Information Mode [enable|disable]
```

```
Security Network DHCP Relay Information Policy [replace|keep|drop]
```

```
Security Network DHCP Relay Statistics [clear]
```

Security Network DHCP Snooping Configuration

```
Security Network DHCP Snooping Mode [enable|disable]
```

```
Security Network DHCP Snooping Port Mode [<port_list>] [trusted|untrusted]
```

```
Security Network DHCP Snooping Statistics [<port_list>] [clear]
```

```
>
```

Each of these commands is explained below.

Command: Show Current DHCP Relay Configuration

Syntax: security network dhcp relay config

Description: Display the current DHCP relay configuration.

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in a standalone device it is always 0). The parameter of "port_no" is the fourth byte and it means the port number. The Remote ID is 6 bytes in length, and the value equals the DHCP relay agents MAC address.

Example: >security network dhcp relay config

```
DHCP Relay Configuration:
```

```
=====
```

```
DHCP Relay Mode           : Disabled
DHCP Relay Server         : NULL
DHCP Relay Information Mode : Disabled
DHCP Relay Information Policy : replace
>
```

Command: Set / Show DHCP Relay Mode

Syntax: security network dhcp relay mode [enable|disable]

Description: Set or show the DHCP relay mode. Per IETF RFC 3046: "DHCP servers unaware of the Relay Agent Information option will ignore the option upon receive and will not echo it back on responses. This is the specified server behavior for unknown options. DHCP servers claiming to support the Relay Agent Information option echo the entire contents of the Relay Agent Information option in all replies." The parameters are:

enable : Enable DHCP relay mode. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. This ensures that the DHCP broadcast message won't be flooded for security considerations. At least one DHCP server must be enabled, configured and running.

disable: Disable DHCP relay mode.

(default: Show flow DHCP relay mode).

Example: >security network dhcp relay mode

```
DHCP Relay Mode           : Disabled
>security network dhcp relay mode enable
We need at least one server
>
```

Command: Set / Show DHCP Relay Server

Syntax: `security network dhcp relay server [<ip_addr>]`

Description: Show or set DHCP relay server, where:

<ip_addr>: IP address (a.b.c.d) of the DHCP relay server. The default is 'Show IP address' of the currently configured and enabled DHCP relay server (if any).

Displays 'NULL' if no DHCP relay server is currently configured.

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain.

Example:

```
>security network dhcp relay server
DHCP Relay Server      : NULL
>security network dhcp relay server 192.168.1.30
>security network dhcp relay server
DHCP Relay Server      : 192.168.1.30
>
```

Command: `Set / Show DHCP Relay Agent Information Option Mode`

Syntax: `security network dhcp relay information mode [enable|disable]`

Description: Set or show DHCP relay agent information option mode.

When you enable DHCP relay information mode operation, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and remote it from a DHCP message when transferring to DHCP client. It only works with DHCP relay operation mode enabled.

The option 82 circuit ID format is "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID (in a standalone device it always 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. The option 82 remote ID value is equal the switch MAC address.

The parameters are:

enable : Enable DHCP relay agent information option mode. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.

disable: Disable DHCP relay agent information option mode.
(default: Show DHCP relay agent information option mode)

Example:

```
>security network dhcp relay information mode
DHCP Relay Information Mode  : Disabled
>security network dhcp relay information mode enable
>security network dhcp relay information mode
DHCP Relay Information Mode  : Enabled
>
```

Command: Set / Show DHCP Relay Information Policy

Syntax: security network dhcp relay information policy [replace|keep|drop]

Description: Set or show the DHCP relay mode. When you enable DHCP relay information mode operation, if the agent receives a DHCP message that already contains relay agent information, it will enforce the policy. The parameters are:

replace : Replace the original relay information when receive a DHCP message that already contains it.

keep : Keep the original relay information when receive a DHCP message that already contains it.

drop : Drop the package when receive a DHCP message that already contains relay information.

(The default is 'Show DHCP relay information policy'.)

Example:

```
>security network dhcp relay information policy
DHCP Relay Information Policy : replace
>security network dhcp relay information policy keep
>security network dhcp relay information policy
DHCP Relay Information Policy : keep
>
```

Command: Show / Clear DHCP Relay Statistics

Syntax: security network dhcp relay statistics [clear]

Description: Show or clear DHCP relay statistics, where:

clear: Clears (resets to zero) all of the DHCP relay statistics.

Example:

```
>security network dhcp relay statistics

Server Statistics:
-----
Transmit to Server      :          0   Transmit Error              :          0
Receive from Server    :          0   Receive Missing Agent Option :          0
Receive Missing Circuit ID :          0   Receive Missing Remote ID   :          0
Receive Bad Circuit ID  :          0   Receive Bad Remote ID       :          0

Client Statistics:
-----
Transmit to Client     :          0   Transmit Error              :          0
Receive from Client    :          0   Receive Agent Option        :          0
Replace Agent Option   :          0   Keep Agent Option           :          0
Drop Agent Option      :          0

>
```

Command: Show Current DHCP Snooping Configuration
Syntax: security network dhcp snooping config
Description: Show the current DHCP snooping configuration.
Example: >security network dhcp snooping config

```
DHCP Snooping Configuration:
=====

DHCP Snooping Mode : Disabled

Port   Port Mode
-----
1      trusted
2      trusted
3      trusted
4      trusted
5      trusted
6      trusted
7      trusted
8      trusted
>
```

Command: Set / Show DHCP Snooping Mode
Syntax: security network dhcp snooping mode [enable|disable]
Description: Set or show the current DHCP snooping mode, where:
enable : Enable DHCP snooping mode. When you enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports.
disable: Disable DHCP snooping mode
(The default is 'Show flow DHCP snooping mode'.)

Example: >security network dhcp snooping mode
DHCP Snooping Mode : Disabled
>security network dhcp snooping mode enable
>security network dhcp snooping mode
DHCP Snooping Mode : Enabled
>

Command: Set / Show DHCP Snooping Port Mode

Syntax: security network dhcp snooping port mode [<port_list>] [trusted|untrusted]

Description: Set or show the current DHCP snooping port mode, where:

<port_list>: Port list or 'All'. The default is 'All' ports.

trusted : Configures the port as trusted sources of the DHCP message (default).

untrusted: Configures the port as untrusted sources of the DHCP message.

(The default is 'Show flow DHCP snooping port mode'.)

Example: >security network dhcp snooping port mode

```
Port  Port Mode
----  -
```

```
1    trusted
```

```
2    trusted
```

```
3    trusted
```

```
4    trusted
```

```
5    trusted
```

```
6    trusted
```

```
7    trusted
```

```
8    trusted
```

```
>security network dhcp snooping port mode 3-5 untrusted
```

```
>security network dhcp snooping port mode
```

```
Port  Port Mode
----  -
```

```
1    trusted
```

```
2    trusted
```

```
3    untrusted
```

```
4    untrusted
```

```
5    untrusted
```

```
6    trusted
```

```
7    trusted
```

```
8    trusted
```

```
>
```

Command: Show / Clear DHCP Snooping Statistics

Syntax: security network dhcp snooping statistics [<port_list>] [clear]

Description: Show or clear DHCP snooping statistics, where:
<port_list>: Port list (1-8) or 'All'. The default is 'All' ports (can be a long display).
clear : Clear DHCP snooping statistics.

Example:

```
>security network dhcp snooping statistics 1
Port 1 Statistics:
-----
Rx Discover:                0    Tx Discover:                0
Rx Offer:                   0    Tx Offer:                   0
Rx Request:                  0    Tx Request:                  0
Rx Decline:                  0    Tx Decline:                  0
Rx ACK:                      0    Tx ACK:                      0
Rx NAK:                      0    Tx NAK:                      0
Rx Release:                  0    Tx Release:                  0
Rx Inform:                   0    Tx Inform:                   0
Rx Lease Query:              0    Tx Lease Query:              0
Rx Lease Unassigned:         0    Tx Lease Unassigned:         0
Rx Lease Unknown:            0    Tx Lease Unknown:            0
Rx Lease Active:             0    Tx Lease Active:             0
>
```

Security Network IP Source Guard Group

IP Source Guard is a security feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic, based on the DHCP Snooping table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

IP source guard checks the IP source address and MAC source address in a packet sent from a host attached to an untrusted access interface on the switch against entries stored in the DHCP snooping database. If IP source guard determines that the packet header contains an invalid source IP address or source MAC address, it keeps the switch from forwarding the packet (the packet is discarded). When you configure IP source guard, you enable on it on one or more VLANs. IP source guard applies its checking rules to packets sent from untrusted access interfaces on those VLANs.

After the DHCP snooping database is populated (via either dynamic DHCP snooping or configuring specific static IP address/MAC address bindings) the IP Source Guard database is built. It then checks incoming packets from access interfaces on the VLANs on which it is enabled. If the source IP addresses and source MAC addresses match the IP Source Guard binding entries, the switch forwards the packets to their specified destination addresses. If they do not match, the packets are discarded.

This group includes the following IP Source Guard commands.

>Security Network IP ?

Available Commands:

Security Network IP Source Guard Configuration

Security Network IP Source Guard Mode [enable|disable]

Security Network IP Source Guard Port Mode [<port_list>] [enable|disable]

Security Network IP Source Guard limit [<port_list>] [<dynamic_entry_limit>|unlimited]

Security Network IP Source Guard Entry [<port_list>] add|delete <vid> <allowed_ip> <allowed_mac>

Security Network IP Source Guard Status [<port_list>]

Security Network IP Source Guard Translation

Each of the IP Source Guard commands is explained below.

Command: Show Current IP Source Guard Configuration

Syntax: security network ip source guard config

Description: Display the current IP Source Guard configuration.

Example: >Security Network IP Source Guard Config

```
IP Source guard Configuration:
=====

IP Source Guard Mode : Enabled

Port   Port Mode   Dynamic Entry Limit
----   -
1      Disabled   unlimited
2      Enabled    1
3      Enabled    2
4      Disabled   unlimited
5      Disabled   unlimited
6      Disabled   unlimited
7      Disabled   unlimited
8      Disabled   unlimited

IP Source Guard Entry Table:

Type    Port  VLAN  IP Address      MAC Address
-----  -
Static  1     1     192.168.1.110  00-00-00-00-00-00
>
```

Command: Set / Show IP Source Guard Mode

Syntax: security network ip source guard mode [enable|disable]

Description: Set or show IP Source Guard mode, where:

enable : Enable IP Source Guard global mode.

disable: Disable IP Source Guard global mode.

Example: >security network ip source guard mode

```
IP Source Guard Mode : Disabled
>security network ip source guard mode enable
>security network ip source guard mode
IP Source Guard Mode : Enabled
>
```

Note that the IP Source Guard function is enabled on a given port only when IP Source Guard is enabled in both Global Mode (via the **security network ip source guard mode** command) and Port Mode (the **security network ip source guard port mode** command). In other words, IP Source Guard must be enabled at the device level (globally) and at the port level (locally) to be fully enabled.

Command: Set / Show IP Source Guard Port Mode

Syntax: security network ip source guard port mode [<port_list>] [enable|disable]

Description: Set or show the IP Source Guard port mode, where:
 <port_list>: Port list or 'all'. The default is 'All' ports.
enable : Enable IP Source Guard for one or more ports.
disable : Disable IP Source Guard for one or more ports.
 (default: Show IP Source Guard port mode)

Example: >security network ip source guard port mode

```

Port   Port Mode
-----
1      Disabled
2      Disabled
3      Disabled
4      Disabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
>security network ip source guard port mode 2-4 enable
>security network ip source guard port mode

Port   Port Mode
-----
1      Disabled
2      Enabled
3      Enabled
4      Enabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
>

```

Note that the IP Source Guard function is enabled on a given port only when IP Source Guard is enabled in both Global Mode (via the **security network ip source guard mode** command) and Port Mode (the **security network ip source guard port mode** command). In other words, IP Source Guard must be enabled at the device level (globally) and at the port level (locally) to be fully enabled.

Command: Set / Show IP Source Guard Limit

Syntax: security network ip source guard limit [<port_list>] [<dynamic_entry_limit>|unlimited]

Description: Set or show the IP Source Guard port limitation for dynamic entries. The parameters are:

<port_list> : Port list or 'All'. The default is 'All' ports.

<dynamic_entry_limit>|unlimited: dynamic entry limit (0-2) or unlimited.

Example:

```
>security network ip source guard limit

Port   Dynamic Entry Limit
-----
1      unlimited
2      unlimited
3      unlimited
4      unlimited
5      unlimited
6      unlimited
7      unlimited
8      unlimited
>security network ip source guard limit 2,3 2
>security network ip source guard limit

Port   Dynamic Entry Limit
-----
1      unlimited
2      2
3      2
4      unlimited
5      unlimited
6      unlimited
7      unlimited
8      unlimited
>
```

Command: Add / Delete IP Source Guard Entry

Syntax: security network ip source guard entry [<port_list>] add|delete <vid> <allowed_ip> <allowed_mac>

Description: Add or delete IP source guard static entry, where:
 <port_list> : Port list or 'all'. The default is 'All' ports.
 add : Add new port IP source guard static entry.
 delete : Delete existing port IP source guard static entry.
 <vid> : VLAN ID (1-4094).
 <allowed_ip> : IP address (a.b.c.d), IP address allowed for doing IP source guard
 <allowed_mac>: MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', where x is a hexadecimal digit); the MAC address allowed for doing IP source guard.

Example:

```
>security network ip source guard entry 4 add 1 192.168.1.30 11.22.33.44.55.66
>
```

Command: Show IP Source Guard Status

Syntax: security network ip source guard status [<port_list>]

Description: Show IP source guard static and dynamic entries, where:
 <port_list>: Port list or 'all'. The default is 'All' ports.

Example: >security network ip source guard status

```
IP Source Guard Entry Table:
```

Type	Port	VLAN	IP Address	MAC Address
Static	4	1	192.168.1.30	11-22-33-44-55-66

```
>
```

Command: Translate IP Source Guard Dynamic to Static

Syntax: security network ip source guard translation

Description: Translate IP source guard dynamic entries into static entries.

Example: >security network ip Source guard translation

```
IP Source Guard:
    Translate 0 dynamic entries into static entries.
>
```

Security Network ARP Inspection Group

ARP Inspection is a security feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. The ARP Inspection feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

The Security Network ARP Inspection group commands are listed below.

>security network arp ?

Available Commands:

Security Network ARP Inspection Configuration

Security Network ARP Inspection Mode [enable|disable]

Security Network ARP Inspection Port Mode [<port_list>] [enable|disable]

Security Network ARP Inspection Entry [<port_list>] add|delete <vid> <allowed_mac> <allowed_ip>

Security Network ARP Inspection Status [<port_list>]

Security Network ARP Inspection Translation

>

The Security Network ARP group commands are explained below.

Command: Show Current ARP Inspection Configuration

Syntax: security network arp inspection config

Description: Display the current ARP inspection parameter settings.

Example: >security network arp inspection config

```

ARP Inspection Configuration:
=====

ARP Inspection Mode : Disabled

Port   Port Mode
----   -
1      Disabled
2      Disabled
3      Disabled
4      Disabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled

ARP Inspection Entry Table:

Type      Port  VLAN  MAC Address          IP Address
-----
Static    1     1     11-22-33-44-55-66   192.168.1.110
Static    1     1     11-22-33-44-55-66   192.168.1.210
Static    2     2     12-34-56-78-87-65   192.168.1.110
>

```

Command: Set / Show ARP Inspection Mode
Syntax: **security network arp inspection mode** [enable|disable]
Description: Set or show ARP inspection mode, where:
enable : Enable ARP Inspection.
disable: Disable ARP Inspection.

Example:

```
>security network arp inspection mode
ARP Inspection Mode : Disabled
>security network arp inspection mode enable
>security network arp inspection mode
ARP Inspection Mode : Enabled
>
```

Note that the ARP Inspection function is enabled on a given port only when ARP Inspection is enabled in both Global mode (via the **security network arp inspection mode** command) and Port mode (the **security network arp inspection port mode** command). In other words, ARP Inspection must be enabled at the device level (globally) and at the port level (locally) to be fully enabled.

Command: Set / Show ARP Inspection Port Mode

Syntax: security network arp inspection port mode [<port_list>] [enable|disable]

Description: Set or show the ARP Inspection port mode, where:
 <port_list>: Port list or 'all'. The default is 'All' ports.
enable : Enable ARP Inspection port.
disable : Disable ARP Inspection port.
 (default: Show ARP Inspection port mode)

Example: >security network arp inspection port mode

```

Port   Port Mode
----   -
1      Disabled
2      Disabled
3      Disabled
4      Disabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
>security network arp inspection port mode 2-4 enable
>security network arp inspection port mode

Port   Port Mode
----   -
1      Disabled
2      Enabled
3      Enabled
4      Enabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
>

```

Note that the ARP Inspection function is enabled on a given port only when ARP Inspection is enabled in both global mode (via the **security network arp inspection mode** command) and Port mode (the **security network arp inspection port mode** command). In other words, ARP Inspection must be enabled at the device level (globally) and at the port level (locally) to be fully enabled.

Command: Add / Delete ARP Inspection Entry

Syntax: **security network arp inspection entry** [<port_list>] add|delete <vid> <allowed_mac> <allowed_ip>

Description: Add or delete ARP inspection static entry, where:
 <port_list> : Port list or 'All'. The default is 'All ports'.
add : Add new port ARP inspection static entry
delete : Delete existing port ARP inspection static entry
 <vid> : VLAN ID (1-4094)
 <allowed_mac>: MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', where x is a hexadecimal digit). This is the MAC address allowed to do ARP request.
 <allowed_ip> : IP address (a.b.c.d). The IP address allowed for doing ARP requests.

Example:

```
>security network arp inspection status
```

ARP Inspection Entry Table:

Type	Port	VLAN	MAC Address	IP Address
------	------	------	-------------	------------

```
>security network arp inspection entry 3-5 add 1 11-22-33-44-55-66 192.168.1.30
```

```
>security network arp inspection status
```

ARP Inspection Entry Table:

Type	Port	VLAN	MAC Address	IP Address
------	------	------	-------------	------------

Static	3	1	11-22-33-44-55-66	192.168.1.30
--------	---	---	-------------------	--------------

Static	4	1	11-22-33-44-55-66	192.168.1.30
--------	---	---	-------------------	--------------

Static	5	1	11-22-33-44-55-66	192.168.1.30
--------	---	---	-------------------	--------------

```
>security network arp inspection entry 3-5 delete 1 11-22-33-44-55-66 192.168.1.10
```

```
>security network arp inspection status
```

ARP Inspection Entry Table:

Type	Port	VLAN	MAC Address	IP Address
------	------	------	-------------	------------

```
>
```

Command: Show Current ARP Inspection Status [<port_list>]
Syntax: security network arp inspection status [<port_list>]
Description: Show ARP inspection static and dynamic entries, where:
 <port_list>: Port list or 'all', default: All ports

Example: >security network arp inspection status 1-4

ARP Inspection Entry Table:

Type	Port	VLAN	MAC Address	IP Address
Static	3	1	11-22-33-44-55-66	192.168.1.30
Static	4	1	11-22-33-44-55-66	192.168.1.30

>security network arp inspection status

ARP Inspection Entry Table:

Type	Port	VLAN	MAC Address	IP Address
Static	3	1	11-22-33-44-55-66	192.168.1.30
Static	4	1	11-22-33-44-55-66	192.168.1.30
Static	5	1	11-22-33-44-55-66	192.168.1.30

>

Command: Translate ARP Inspection Entries
Syntax: security network arp inspection translation
Description: Translate ARP inspection dynamic entries into static entries.
Example: >security network arp inspection translation

ARP Inspection:

Translate 0 dynamic entries into static entries.

>

Security > AAA Commands

The S3280 supports Security **AAA** (Authentication, Authorization, Accounting) commands for RADIUS and TACACS+.

RADIUS (Remote Authentication Dial In User Service) is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

TACACS+ (Terminal Access Controller Access Control System Plus) is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Caution: Before enabling Radius or TACACS+, make sure that the related AAA server is operational and that at least the AAA server's IP address/hostname and encryption/decryption key parameters are set correctly. Make sure you are using the safe method:

1. Open a CLI session.
2. Enter the command "**security aaa config**".
3. Try to open a Telnet session.

Now, if the attempt fails (possibly because of an incorrect AAA parameter setting) access to the CLI agent is retained (via the CLI session) and any AAA parameter setting can be corrected in the CLI session.

These CLI command setting are common for all of the Authentication Servers.

The available S3280 Security **AAA** commands include:

>**security aaa ?**

Available Commands:

Security AAA Configuration

Security AAA Timeout [<timeout>]

Security AAA Deadtime [<dead_time>]

Security AAA RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Security AAA ACCT_RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Security AAA TACACS+ [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Security AAA Statistics [<server_index>]

The S3280 Security **AAA** commands are explained below.

Command: Show Current AAA Configuration

Syntax: security aaa config

Description: Show the current Authentication and Accounting configuration.

Example:

```
>security aaa config

AAA Configuration:
=====

Server Timeout      : 15 seconds

Server Dead Time   : 300 seconds

RADIUS Authentication Server Configuration:
=====
Server  Mode      IP Address      Secret          Port
-----  -
1       Disabled
2       Disabled
3       Disabled
4       Disabled
5       Disabled
1812
1812
1812
1812
1812

RADIUS Accounting Server Configuration:
=====
Server  Mode      IP Address      Secret          Port
-----  -
1       Disabled
2       Disabled
3       Disabled
4       Disabled
5       Disabled
1813
1813
1813
1813
1813

TACACS+ Authentication Server Configuration:
=====
Server  Mode      IP Address      Secret          Port
-----  -
1       Disabled
2       Disabled
3       Disabled
4       Disabled
5       Disabled
49
49
49
49
49

>
```

Command: Set / Show AAA Timeout

Syntax: security aaa timeout [<timeout>]

Description: Set or show the server timeout period.

Timeout can be set to a number from 3 to 3600 seconds; it is the maximum time to wait for a reply from a server. If the server does not reply within this timeframe, the S3280 considers it to be 'dead' and continues with the next enabled server (if any).

RADIUS servers use the UDP protocol, which is less reliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be 'dead'.

The parameters are:

<timeout>: Server response timeout (3-3600 seconds).

(default: Show server timeout configuration).

```
Example: >security aaa timeout
Server Timeout      : 15 seconds
>security aaa timeout 30
>security aaa timeout
Server Timeout      : 30 seconds
>
```

Command: Set / Show AAA Deadtime

Syntax: security aaa deadtime [<dead_time>]

Description: Set or show server dead time

Dead Time can be set to a number from 0 to 3600 seconds; it is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as 'dead'. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. The parameters are:

<dead_time>: Time that a server is considered dead if it doesn't answer a request. The valid range is 0-3600 seconds. The default is 300 seconds.

(default: Show server dead time configuration).

```
Example: >security aaa deadtime
Server Dead Time   : 300 seconds
>security aaa deadtime 600
>security aaa deadtime
Server Dead Time   : 600 seconds
>
```

Command: Set / Show AAA RADIUS Server Setup

Syntax: security aaa radius [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>]
[<server_port>]

Description: Set or show RADIUS authentication server setup. The parameters are:

<server_index> :The AAA RADIUS server index (1-5).

(default: Show RADIUS authentication server configuration)

enable : Enable RADIUS authentication server

disable : Disable RADIUS authentication server

(default: Show RADIUS server mode)

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

<secret> : Secret shared with external authentication server. To use spaces in secret, enquote the secret. Quotes within the secret are not allowed.

<server_port> : Server UDP port. Use 0 to use the default RADIUS port (1812).

Example:

```
>security aaa radius
```

```
RADIUS Authentication Server Configuration:
```

```
=====
```

Server	Mode	IP Address	Secret	Port
1	Disabled			1812
2	Disabled			1812
3	Disabled			1812
4	Disabled			1812
5	Disabled			1812

```
>
```

Command: Set / Show AAA ACCT_RADIUS Server Setup

Syntax: security aaa acct_radius [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Description: Set or show RADIUS accounting server setup, where:
 The AAA Accounting RADIUS server index (1-5).
 (default: Show RADIUS accounting server configuration).
enable : Enable RADIUS accounting server
disable : Disable RADIUS accounting server
 (default: Show RADIUS server mode)
<ip_addr_string>: IP host address (a.b.c.d) or a host name string
<secret> : Secret shared with external accounting server. To use spaces in secret, enquote the secret. Quotes within the secret are not allowed. Up to 29 characters are allowed.
<server_port> : Server UDP port. Use 0 to use the default RADIUS port (1813).

Example:

```
>security aaa acct_radius

RADIUS Accounting Server Configuration:
=====
Server  Mode      IP Address      Secret          Port
-----  -
1       Disabled    192.168.1.30    Buffrey1 1      1813
2       Disabled    192.168.1.30    Buffrey1 2      1813
3       Disabled    192.168.1.30    Buffrey1 3      1813
4       Disabled    192.168.1.30    Buffrey1 4      1813
5       Disabled    192.168.1.30    Buffrey1 5      1813
>
>security aaa acct_radius 1 enable 192.168.1.30 Buffrey1 1
>security aaa acct_radius 2 enable 192.168.1.30 Buffrey1 2
>security aaa acct_radius

RADIUS Accounting Server Configuration:
=====
Server  Mode      IP Address      Secret          Port
-----  -
1       Enabled   192.168.1.30    *****      1
2       Enabled   192.168.1.30    *****      2
3       Disabled  192.168.1.30    *****      1813
4       Disabled  192.168.1.30    *****      1813
5       Disabled  192.168.1.30    *****      1813
>
```

Command: Set / Show AAA TACACS+ Server Setup

Syntax: security aaa tacacs+ [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Description: Set or show TACACS+ authentication server setup. The parameters are:

<server_index> :The server index (1-5).

(default: Show TACACS+ authentication server configuration).

enable : Enable TACACS+ authentication server.

disable : Disable TACACS+ authentication server.

(The default is 'Show TACACS+ server mode'.)

<ip_addr_string>: IP host address (a.b.c.d) or a host name string.

<secret> : Secret shared with external authentication server. To use spaces in secret, enquote the secret. Quotes within the secret are not allowed. Up to 29 characters.

<server_port> : Server TCP port. Enter 0 to use the default TACACS+ port (49).

Example:

```
>security aaa tacacs+
```

```
TACACS+ Authentication Server Configuration:
```

Server	Mode	IP Address	Secret	Port
1	Disabled			49
2	Disabled			49
3	Disabled			49
4	Disabled			49
5	Disabled			49

```
>security aaa tacacs+ 1 enable 192.168.1.30 Buffrey1 0
```

```
>security aaa tacacs+
```

```
TACACS+ Authentication Server Configuration:
```

Server	Mode	IP Address	Secret	Port
1	Enabled	192.168.1.30	*****	49
2	Disabled			49
3	Disabled			49
4	Disabled			49
5	Disabled			49

```
>
```

```
>security aaa tacacs+ 2 enable 192.168.1.31 Buffrey1 2
```

```
>security aaa tacacs+
```

```
TACACS+ Authentication Server Configuration:
```

Server	Mode	IP Address	Secret	Port
1	Enabled	192.168.1.30	*****	49
2	Enabled	192.168.1.31	*****	2
3	Disabled			49
4	Disabled			49
5	Disabled			49

Command: Show Current AAA Statistics

Syntax: security aaa statistics [<server_index>]

Description: Show current RADIUS statistics, where:
<server_index> : The RADIUS server index number (1-5).
(The default is 'Show statistics for all servers').

Example:

```
>security aaa statistics 1

Server #1 (0.0.0.0:1812) RADIUS Authentication Statistics:
Rx Access Accepts:                0    Tx Access Requests:                0
Rx Access Rejects:                0    Tx Access Retransmissions:        0
Rx Access Challenges:             0    Tx Pending Requests:              0
Rx Malformed Acc. Responses:      0    Tx Timeouts:                      0
Rx Bad Authenticators:            0
Rx Unknown Types:                 0
Rx Packets Dropped:               0
State:                            Disabled
Round-Trip Time:                  0 ms

Server #1 (0.0.0.0:1813) RADIUS Accounting Statistics:
Rx Responses:                     0    Tx Requests:                      0
Rx Malformed Responses:           0    Tx Retransmissions:               0
Rx Bad Authenticators:            0    Tx Pending Requests:              0
Rx Unknown Types:                 0    Tx Timeouts:                      0
Rx Packets Dropped:               0
State:                            Disabled
Round-Trip Time:                  0 ms
>
```

STP Commands

The S3280 supports an array of STP (Spanning Tree Protocol) CLI commands. STP is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN.

The S3280 supports the spanning tree protocols of STP/RSTP and MSTP on all interfaces. The Spanning Tree protocols help in creating a loop free bridged network. The implementation conforms to the IEEE specs 802.1D for STP, 802.1w for RSTP and 802.1s for MSTP.

The S3280 can act in the role of a root bridge or as a designated bridge by the process of election. The priorities for the bridge instance that is used in BPDU frames can be configured. For MSTP, each MSTI (Multiple Spanning Tree Instance) priority can be configured for the Common and Internal Spanning Tree (CIST) instance.

The MSTP protocol version works over VLAN instances, and multiple VLANs can be added to an MSTI; however, at any time a VLAN can be only be part of one MSTI. Configuration for each MSTI and the VLANs that belong to that instance is supported. The S3280 also supports configuration options for enabling/disabling BPDU guard, path cost for that port, restricting topology change notification, etc. Note that MSTP is disabled on the S3280 MGMT port (port 9).

These S3280 commands provide STP functions.

```
>stp ?
```

Available Commands:

STP Configuration

```
STP Version [<stp_version>]
STP Txhold [<holdcount>]
STP MaxHops [<maxhops>]
STP MaxAge [<max_age>]
STP FwdDelay [<delay>]
STP CName [<config-name>] [<integer>]
STP bpduFilter [enable|disable]
STP bpduGuard [enable|disable]
STP recovery [<timeout>]
STP Status [<msti>] [<port_list>]
STP Msti Priority [<msti>] [<priority>]
STP Msti Map [<msti>] [clear]
STP Msti Add <msti> <vid>
STP Port Configuration [<port_list>]
STP Port Mode [<port_list>] [enable|disable]
STP Port Edge [<port_list>] [enable|disable]
STP Port AutoEdge [<port_list>] [enable|disable]
STP Port P2P [<port_list>] [enable|disable|auto]
STP Port RestrictedRole [<port_list>] [enable|disable]
STP Port RestrictedTcn [<port_list>] [enable|disable]
STP Port bpduGuard [<port_list>] [enable|disable]
STP Port Statistics [<port_list>] [clear]
STP Port Mcheck [<port_list>]
STP Msti Port Configuration [<msti>] [<port_list>]
STP Msti Port Cost [<msti>] [<port_list>] [<path_cost>]
STP Msti Port Priority [<msti>] [<port_list>] [<priority>]
>
```

The available STP commands are explained below.

Command: Show Current STP Configuration

Syntax: stp configuration

Description: Displays the current S3280 configuration setup. Note that MSTP is disabled on the S3280 MGMT port.

Example: >stp config

```
STP Configuration:
=====

Protocol Version: MSTP
Max Age           : 11
Forward Delay     : 11
Tx Hold Count     : 1
Max Hop Count     : 10
BPDU Filtering    : Enabled
BPDU Guard        : Enabled
Error Recovery    : 55 seconds
>
```

Command: Set / Show STP Version

Syntax: stp version [<stp_version>]

Description: Set or show the STP Bridge protocol version, where <stp_version>: mstp|rstp|stp. Note that MSTP is disabled on the S3280 MGMT port. The parameters are:

mstp: configures the Multiple Spanning Tree protocol.

rstp: configures the Rapid Spanning Tree protocol.

stp: configures the Spanning Tree protocol.

Example: STP>version

```
Protocol Version: Compatible (STP)
STP>version rstp
STP>version
Protocol Version: RSTP
STP>version mstp
STP>version
Protocol Version: MSTP
STP>
```

Command: Set / Show STP Txhold Count

Syntax: stp txhold [<holdcount>]

Description: Set or show the STP Bridge Transmit Hold Count parameter. The number of BPDUs a port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are 1 - 10 BPDUs per second. The default is 6 BPDUs / second.

The parameters are:

<holdcount>: The number of BPDUs a port can send per second. (1-10 BPDU's per second).

Example: STP>txhold 3

```
STP>txhold
Tx Hold Count   : 3
STP>
```


Command: Set / Show STP Max Hops

Syntax: stp maxhops [<maxhops>]

Description: Sets or shows the MSTP Bridge Max Hop Count parameter, where:
<maxhops>: STP BPDU Maximum number of Hops (6-40).

Example:

```
STP>maxhops 5
Invalid parameter: 5

Syntax:
STP MaxHops [<maxhops>]
STP>maxhops 20
STP>maxhops
Max Hop Count      : 20
STP>
```

Command: Set / Show STP Max Age

Syntax: stp maxage [<max_age>]

Description: Sets or shows the bridge instance maximum age. This is the maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are 6 to 40 seconds, and MaxAge must be $\leq (\text{FwdDelay}-1)*2$. The parameters are:

<max_age>: STP maximum age time (6-39, and max_age $\leq (\text{forward_delay}-1)*2$)

Example:

```
STP>maxage 4
Invalid parameter: 4

Syntax:
STP MaxAge [<max_age>]
STP>maxage 40
Invalid parameter: 40

Syntax:
STP MaxAge [<max_age>]
STP>maxage 20
STP>maxage
Max Age            : 20
STP>
```

Command: Set / Show STP Forward Delay

Syntax: stp fwddelay [<delay>]

Description: Set or show the bridge instance forward delay. This is the delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds. The parameters are:

<delay>: MSTP forward delay (4-30, and max_age $\leq (\text{forward_delay}-1)*2$)

Example:

```
STP>fwddelay 30
STP>fwddelay
Forward Delay      : 30
STP>
```

Command: Set / Show STP Config Name

Syntax: **stp cname** [<config-name>] [<integer>]

Description: Set or show MSTP configuration name and revision, where:
 <config-name>: For the MSTP Configuration name, enter a text string up to 32 characters long. Use quotes (") to embed spaces in name.
 <integer> : Integer value

Example:

```
STP>cname *STP"cfg1 1
STP>cname
Configuration name: *STP"cfg1 1
Configuration rev.: 0
STP>
```

Command: Set / Show STP BPDU Filter

Syntax: **stp bpdupfilter** [enable|disable]

Description: Edge Port BPDU Filtering controls whether a port explicitly configured as Edge will transmit and receive BPDUs. Set or show edge port BPDU Filtering, where:
enable|disable: enable or disable BPDU Filtering for Edge ports.

Example:

```
STP>bpdupfilter enable
STP>bpdupfilter
BPDU Filtering : Enabled
STP>
```

Command: Set / Show STP BPDU Guard

Syntax: **stp bpduguard** [enable|disable]

Description: Edge Port BPDU Guard controls whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology. Set or show edge port BPDU Guard, where:
enable|disable: enables or disables BPDU Guard for Edge ports.

Example:

```
>stp bpduguard
BPDU Guard : Disabled
>stp bpduguard enable
>stp bpduguard
BPDU Guard : Enabled
>
```

Command: Set / Show STP Recovery

Syntax: **stp recovery** [<timeout>]

Description: Set or show edge port error recovery timeout, where:
 <timeout>: Time before error-disabled ports are re-enabled (30-86400 seconds, 0 disables). (The default is 'Show recovery timeout'.)

Example:

```
STP>recovery 30
STP>recovery
Error Recovery : 30 seconds
STP>recovery 3000
STP>recovery
Error Recovery : 3000 seconds
STP>
```

Command: Show STP Status

Syntax: **stp status** [<msti>] [<port_list>]

Description: Display the current STP Bridge status, where:

<msti> : STP bridge instance number (0-7, CIST=0, MSTI1=1, ...).

<port_list>: Port list or 'All'. The default is 'All' ports.

Example:

```
>stp status
CIST Bridge STP Status
Bridge ID      : 32768.00-C0-F2-00-00-01
Root ID       : 32768.00-C0-F2-00-00-01
Root Port     : -
Root PathCost: 0
Regional Root: 32768.00-C0-F2-00-00-01
Int. PathCost: 0
Max Hops      : 20
TC Flag       : Steady
TC Count      : 0
TC Last       : -
Port          Port Role      State      Pri PathCost Edge P2P Uptime
-----
1 DesignatedPort Forwarding 128 200000 Yes Yes 0d 00:42:57
>
```

Command: **Set / Show STP MSTI Priority**

Syntax: **stp msti priority** [<msti>] [<priority>]

Description: This command lets you view / modify the current STP MSTI bridge instance priority configuration. Set or show the bridge instance priority. An MSTI (Multiple Spanning Tree Instance) is typically one of the uplink ports that connects to one of the gateway devices. MSTI information can include VLAN mapping, bridge priority, port priority, and cost. The parameters are:

<msti> : STP bridge instance number (0-7, CIST=0, MSTI1=1, ...). 'MSTI' is the bridge instance. The CIST is the default instance, which is always active.

<priority>: STP bridge priority (0/4096/8192/12288/.../53248/57344/61440). This 'Priority' controls the bridge priority. A lower numeric values gives better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

```
Example: >stp msti priority 0 8192
>stp msti priority 1 12288
>stp msti priority
MSTI# Bridge Priority
-----
CIST 8192
MSTI1 12288
MSTI2 32768
MSTI3 32768
MSTI4 32768
MSTI5 32768
MSTI6 32768
MSTI7 32768
>
```

Command: Show / Clear STP MSTI Mapping

Syntax: **stp msti map** [<msti>] [clear]

Description: Show or clear MSTP MSTI VLAN mapping configuration, where:
<msti>: STP bridge instance number (0-7, CIST=0, MSTI1=1, ...).
clear : Clear VID-to-MSTI mapping.

```
Example: >stp msti map
MSTI   VLANs mapped to MSTI
-----
MSTI1  1
MSTI2  2
MSTI3  3-5
MSTI4  6-8
MSTI5  No VLANs mapped
MSTI6  No VLANs mapped
MSTI7  No VLANs mapped
>stp msti map clear
Mapping all VLANs to CIST
>stp msti map
MSTI   VLANs mapped to MSTI
-----
MSTI1  No VLANs mapped
MSTI2  No VLANs mapped
MSTI3  No VLANs mapped
MSTI4  No VLANs mapped
MSTI5  No VLANs mapped
MSTI6  No VLANs mapped
MSTI7  No VLANs mapped
>
```

Command: STP MSTI Add VLAN

Syntax: `stp msti add <msti> <vid>`

Description: Add a VLAN to a MSTI, where:

<msti>: The STP bridge instance number to be added (0-7, CIST=0, MSTI1=1, ...).

<vid>: VLAN ID (1-4094).

Note: use the `stp msti map` command to display the updated configuration.

Example:

```
>stp msti map
MSTI  VLANs mapped to MSTI
-----
MSTI1  No VLANs mapped
MSTI2  No VLANs mapped
MSTI3  No VLANs mapped
MSTI4  No VLANs mapped
MSTI5  No VLANs mapped
MSTI6  No VLANs mapped
MSTI7  No VLANs mapped
>stp msti add 1 1
Add VLAN 1 to MSTI1
>stp msti add 2 3
Add VLAN 3 to MSTI2
>stp msti map
MSTI  VLANs mapped to MSTI
-----
MSTI1  1
MSTI2  3
MSTI3  No VLANs mapped
MSTI4  No VLANs mapped
MSTI5  No VLANs mapped
MSTI6  No VLANs mapped
MSTI7  No VLANs mapped
>
```

Command: Show Current STP Port Configuration

Syntax: `stp port config [<port_list>]`

Description: Show the current STP Port configuration, where:

<port_list>: Port list or 'all'. Port zero (0) means aggregations.

Example:

`>stp port config`

Port	Mode	AdminEdge	AutoEdge	restrRole	restrTcn	Point2point
Aggr	Enabled	Disabled	Enabled	Disabled	Disabled	Enabled
Port	Mode	AdminEdge	AutoEdge	restrRole	restrTcn	Point2point
1	Enabled	Disabled	Enabled	Disabled	Disabled	Auto
2	Enabled	Disabled	Enabled	Disabled	Disabled	Auto
3	Enabled	Disabled	Enabled	Disabled	Disabled	Auto
4	Enabled	Disabled	Enabled	Disabled	Disabled	Auto
5	Enabled	Disabled	Enabled	Disabled	Disabled	Auto
6	Enabled	Disabled	Enabled	Disabled	Disabled	Auto
7	Enabled	Disabled	Enabled	Disabled	Disabled	Auto
8	Enabled	Disabled	Enabled	Disabled	Disabled	Auto

Command: Set / Show STP Port Mode

Syntax: **stp port mode** [<port_list>] [enable|disable]

Description: Set or show the STP enabling for a port, where:
<port_list>: Port list or 'all'. Port zero (0) means aggregations.
enable : Enable MSTP protocol.
disable: Disable MSTP protocol.

Example:

```
>stp port mode
Port  Mode
----  -
Aggr  Enabled

Port  Mode
----  -
1     Enabled
2     Enabled
3     Enabled
4     Enabled
5     Enabled
6     Enabled
7     Enabled
8     Enabled
>stp port mode 2,3 disable
>stp port mode
Port  Mode
----  -
Aggr  Enabled

Port  Mode
----  -
1     Enabled
2     Disabled
3     Disabled
4     Enabled
5     Enabled
6     Enabled
7     Enabled
8     Enabled
>
```

Command: Set / Show STP Port Edge

Syntax: `stp port edge [<port_list>] [enable|disable]`

Description: Set or show the STP adminEdge port parameter, where:
 <port_list>: Port list or 'all'. The default is 'All' ports.
enable : Configure MSTP adminEdge to Edge.
disable: Configure MSTP adminEdge to Non-edge.

Example: `>stp port edge`

```

Port   AdminEdge
-----
Aggr   Disabled

Port   AdminEdge
-----
1      Disabled
2      Disabled
3      Disabled
4      Disabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
>stp port edge 2,3 enable
>stp port edge
>stp port edge

Port   AdminEdge
-----
Aggr   Enabled

Port   AdminEdge
-----
1      Disabled
2      Enabled
3      Enabled
4      Disabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
>

```

Command: Set / Show STP Port AutoEdge

Syntax: **stp port autoedge** [<port_list>] [enable|disable]

Description: AutoEdge controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port.

Set or show the STP autoEdge port parameter, where:

<port_list>: Port list or 'all'. The default is All ports.

enable : Enable MSTP AutoEdge.

disable: Disable MSTP AutoEdge.

Example:

```
STP>port autoedge 1 disable
STP>port autoedge 2 disable
STP>port autoedge

Port  AutoEdge
----  -
Aggr  Disabled

Port  AutoEdge
----  -
1     Disabled
2     Disabled
3     Enabled
4     Enabled
5     Enabled
6     Enabled
7     Enabled
8     Enabled
STP>
```


Command: Set / Show STP Port P2P

Syntax: **stp port p2p** [<port_list>] [enable|disable|auto]

Description: Port Point2Point (P2P) controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true (enabled) or false. The transition to the forwarding state is faster for point-to-point LANs than for shared media.

Set or show the STP point2point port parameter, where:

<**port_list**>: Port list or 'All'. The default is 'All' ports.

enable : Enable MSTP point2point.

disable: Disable MSTP point2point.

auto : Automatic MSTP point2point detection configured (the default).

Example:

```
>stp port p2p

Port   Point2point
----   -
Aggr   Enabled

Port   Point2point
----   -
1      Auto
2      Auto
3      Auto
4      Auto
5      Auto
6      Auto
7      Auto
8      Auto
>stp port p2p 1,2 enable
>stp port p2p 3 disable
>stp port p2p

Port   Point2point
----   -
Aggr   Disabled

Port   Point2point
----   -
1      Enabled
2      Enabled
3      Disabled
4      Auto
5      Auto
6      Auto
7      Auto
8      Auto
>
```

Command: Set / Show STP Port Restricted Role

Syntax: `stp port restrictedrole [<port_list>] [enable|disable]`

Description: Restricted Role, if enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause a lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as 'Root Guard'.

Set or show the MSTP '*restrictedRole*' port parameter, where:

<port_list>: Port list or 'all', default: All ports.

enable : Enable MSTP restricted role.

disable: Disable MSTP restricted role.

```

Example: >stp port restrictedrole

Port  restrRole
----  -
Aggr  Disabled

Port  restrRole
----  -
1     Disabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
>stp port restrictedrole 1,2 enable
>stp port restrictedrole

Port  restrRole
----  -
Aggr  Enabled

Port  restrRole
----  -
1     Enabled
2     Enabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
>

```

Command: Set / Show STP Port Restricted TCN

Syntax: `stp port restrictedtcn [<port_list>] [enable|disable]`

Description: Restricted TCN, If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

Set or show the MSTP *restrictedTcn* port parameter, where:

<port_list>: Port list or 'all', default: All ports.

enable : Enable MSTP restricted TCN.

disable: Disable MSTP restricted TCN

Example:

```
STP>port restrictedtcn 1 enable
STP>port restrictedtcn 3 enable
STP>port restrictedtcn
```

```
Port   restrTcn
----  -
Aggr   Enabled

Port   restrTcn
----  -
1      Enabled
2      Disabled
3      Enabled
4      Disabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
STP>
```

Command: Set / Show STP Port BPDUGuard

Syntax: `stp port bpduguard [<port_list>] [enable|disable]`

Description: BPDUGuard, if enabled, causes the S3280 port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port **Edge** status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

Set or show the bpduguard port parameter, where:

<port_list>: Port list or 'all', default: All ports.

enable : Enable port BPDUGuard.

disable: Disable port BPDUGuard.

Example: STP>`port bpduguard 1 enable`
 STP>`port bpduguard 3 enable`
 STP>`port bpduguard`

Port bpduguard

Aggr Enabled

Port bpduguard

1 Enabled

2 Disabled

3 Enabled

4 Disabled

5 Disabled

6 Disabled

7 Disabled

8 Disabled

STP>

Command: Show / Clear STP Port Statistics

Syntax: `stp port statistics [<port_list>] [clear]`

Description: Show or clear the STP port statistics, where:

<port_list>: Port list or 'All'. The default is 'All' ports.

clear : Clear the selected port statistics.

Example:

STP>`port statistics`

Port	Rx MSTP	Tx MSTP	Rx RSTP	Tx RSTP	Rx STP	Tx STP	Rx TCN	Tx TCN	Rx Ill.	Rx Unk.
4	0	8992	0	13	0	28	0	0	0	0

STP>`port statistics clear`

Port	Rx MSTP	Tx MSTP	Rx RSTP	Tx RSTP	Rx STP	Tx STP	Rx TCN	Tx TCN	Rx Ill.	Rx Unk.
4	0	0	0	0	0	0	0	0	0	0

STP>`port statistics`

Port	Rx MSTP	Tx MSTP	Rx RSTP	Tx RSTP	Rx STP	Tx STP	Rx TCN	Tx TCN	Rx Ill.	Rx Unk.
4	0	1	0	0	0	0	0	0	0	0

STP>

Command: **Set STP Port Migration Check**

Syntax: **stp port mcheck** [<port_list>]

Description: Set the STP mCheck (Migration Check) variable for ports. If a port running MSTP (or RSTP) connects to a bridge running STP, this port will automatically migrate to STP-compatible mode. However, it can not automatically migrate back to the MSTP (or RSTP) mode, but rather it will remain in STP-compatible mode if:

- * The bridge running STP is shut down or removed.
- * The bridge running STP migrates to the MSTP (or RSTP) mode.

Then you can perform an mCheck (Migration Check) operation to force the port to migrate to the MSTP (or RSTP) mode.

The parameters are:

<port_list>: Port list or 'All'. The default is All ports.

Example:

```
STP>port mcheck 1
STP>port mcheck all
STP>
```

Command: **Show Current STP MSTI Port Configuration**

Syntax: **stp msti port configuration** [<msti>] [<port_list>]

Description: Show the STP port instance configuration, where:

<msti> : STP bridge instance number (0-7, CIST=0, MSTI1=1, ...).

<port_list>: Port list or 'All'. The default is 'All' ports.

Example:

```
STP>msti port config

MSTI  Port  Path Cost  Priority
----  -
CIST  Aggr  Auto       128

MSTI  Port  Path Cost  Priority
----  -
CIST  1     Auto       128
CIST  2     Auto       128
CIST  3     Auto       128
CIST  4     Auto       128
CIST  5     Auto       128
CIST  6     Auto       128
CIST  7     Auto       128
CIST  8     Auto       128
STP>
```

Command: Set / Show STP MSTI Port Cost

Syntax: `stp msti port cost [<msti>] [<port_list>] [<path_cost>]`

Description: Set or show the STP port instance path cost, where:
 <msti> : STP bridge instance number (0-7, CIST=0, MSTI1=1, ...).
 <port_list>: Port list or 'all'. Port zero (0) means aggregations.
 <path_cost>: STP port path cost (1-200000000) or 'auto'.

Example: `STP>msti port cost 0 1 500000`

```
STP>msti port cost
MSTI  Port  Path Cost
----  ----  -
CIST  Aggr  Auto

MSTI  Port  Path Cost
----  ----  -
CIST  1    500000
CIST  2    Auto
CIST  3    Auto
CIST  4    Auto
CIST  5    Auto
CIST  6    Auto
CIST  7    Auto
CIST  8    Auto
STP>
```

Command: Set / Show STP MSTI Port Priority

Syntax: `stp msti port priority [<msti>] [<port_list>] [<priority>]`

Description: The 'Priority' controls the port priority of ports having identical port cost.
 Set or show the STP port instance priority, where:
 <msti> : STP bridge instance number (0-7, CIST=0, MSTI1=1, ...).
 <port_list>: Port list or 'all'. Port zero means aggregations.
 <priority> : STP port priority (0/16/32/48/.../224/240).

Example: `STP>msti port priority 0 1 32`

```
STP>msti port priority 0 2 64
STP>msti port priority
MSTI  Port  Priority
----  ----  -
CIST  Aggr  128

MSTI  Port  Priority
----  ----  -
CIST  1    32
CIST  2    64
CIST  3    128
CIST  4    128
CIST  5    128
CIST  6    128
CIST  7    128
CIST  8    128
STP>
```

Aggr (Aggregation) Commands

Aggr (aggregation) involves using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability (e.g., port aggregation, link aggregation).

These S3280 commands provide Link Aggregation (Aggr) functions:

>**aggr ?**

Available Commands:

Aggr Configuration

Aggr Add <port_list> [<aggr_id>]

Aggr Delete <aggr_id>

Aggr Lookup [<aggr_id>]

Aggr Mode [smac|dmac|ip|port] [enable|disable]

>

The S3280 Link Aggregation (Aggr) commands are explained below.

Command: **Show Current Aggr Configuration**

Syntax: **aggr>configuration** or **>aggr configuration**

Description: Displays the current link aggregation configuration in terms of SMAC, DMAC, IP and Port.

Example: **>aggr config**

```
Aggregation Configuration:
```

```
=====
```

```
Aggregation Mode:
```

```
SMAC   : Enabled
```

```
DMAC   : Disabled
```

```
IP     : Enabled
```

```
Port   : Enabled
```

```
>
```

Command: Add / Modify Aggregation ID

Syntax: aggr add <port_list> [<aggr_id>]

Description: Add or modify link aggregation, where:

<port_list>: Port list or 'All'. The default is 'All' ports.

<aggr_id> : Aggregation ID: 1 (the number of supported ports divided by 2).

Note: use the **aggr lookup** or **aggr config** command to view the configuration changes.

Example:

```
>aggr add 2,3,4 2
>aggr config

Aggregation Configuration:
=====

Aggregation Mode:

SMAC   : Enabled
DMAC   : Disabled
IP     : Enabled
Port   : Enabled

Aggr ID  Name      Type      Configured Ports  Aggregated Ports
-----  -
2        LLAG2    Static    2-4                None
>aggr lookup

Aggr ID  Name      Type      Configured Ports  Aggregated Ports
-----  -
2        LLAG2    Static    2-4                None
>aggr add 2,3,4 2
>aggr lookup

Aggr ID  Name      Type      Configured Ports  Aggregated Ports
-----  -
2        LLAG2    Static    2-4                None
>
```

If you try to aggregate a port in more than one Aggregation ID, a message such as “Port 2 is already included in aggregation 2” displays.

If you use this command to add or modify link aggregation and STP is enabled, the message “802.IX is enabled on one or more ports in the aggregation” displays.

Command: Delete Existing Aggregation

Syntax: `aggr delete <aggr_id>`

Description: Delete an existing link aggregation, where:
 <aggr_id>: Aggregation ID: 1 (the number of frontports divided by 2).

Example:

```
>aggr delete 2
>aggr lookup
>
>aggr lookup
>aggr add 2,3,4 2
>aggr lookup

Aggr ID  Name      Type      Configured Ports  Aggregated Ports
-----  -
2         LLAG2     Static    2-4                None
>aggr delete 2
>aggr lookup
>
```

Messages: *The aggregation does not exist*

Command: Lookup (Display) Current Aggregation Config

Syntax: `aggr lookup [<aggr_id>]`

Description: Displays the current link aggregation configuration of a port in terms of its ID, Name, Type, Configured Ports, and Aggregated Ports.

Example:

```
>aggr add 2,3 1
>aggr lookup

Aggr ID  Name      Type      Configured Ports  Aggregated Ports
-----  -
1         LLAG1     Static    2,3                None
>
```

Command: Set / Show Aggregation Mode

Syntax: `aggr mode [smac|dmac|ip|port] [enable|disable]`

Description: This command is used to configure the Aggregation hash mode and the aggregation group. Define or display the link aggregation traffic distribution mode, where:
smac = Source MAC address.
dmac = Destination MAC address.
ip = Source and destination IP address.
port = Source and destination UDP port.
enable = Enable field in traffic distribution.
disable = Disable field in traffic distribution.

Example:

```
>aggr mode
Aggregation Mode:
SMAC   : Enabled
DMAC   : Disabled
IP     : Enabled
Port   : Enabled
>aggr mode smac disable
>aggr mode dmac enable
>aggr mode
Aggregation Mode:
SMAC   : Disabled
DMAC   : Enabled
IP     : Enabled
Port   : Enabled
>
```

The Hash Code Contributors include the TCP/UDP Port Number, IP Address, Destination MAC Address, and the Source MAC Address, where:

Source MAC Address: can be used to calculate the destination port for the frame. Enable to use the Source MAC address, or disable. By default, Source MAC Address (SMAC) is enabled.

Destination MAC Address: can be used to calculate the destination port for the frame. Enable to use the Destination MAC Address. By default, Destination MAC Address (DMAC) is disabled.

IP Address: can be used to calculate the destination port for the frame. Enable for the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.

TCP/UDP Port Number: can be used to calculate the destination port for the frame. Enable to use the TCP/UDP Port Number. By default, TCP/UDP Port Number is enabled.

LACP Commands

LACP is the IEEE 802.3ad Link Aggregation Control Protocol that allows bundling several physical ports together to form a single logical port.

The S3280 supports Link aggregation per IEEE 802.1AX-2008. The Link aggregation supports several physical links bundled into a single logical link for resiliency and load sharing. The S3280 uses LACP PDUs to negotiate with peer devices and to exchange information about the links to be bundled automatically when enabled on the physical port.

The resolved aggregation status and peer information status are available. The load sharing mechanism uses all the physical links to transfer the traffic, but for a flow only one link can be used to make sure the packets are sent/received in order. It uses a hash function to determine which port should carry a traffic flow. The device lets you choose the fields that are needed for generating the hash code needed for routing a flow through a single physical port belonging to the aggregate group.

LACP takes care of link failures where if one link fails the flows belonging to that link are transferred to another link based on the hash mechanism which needs to choose from the available links. The static aggregation option is also supported so the S3280 will work with devices which don't support LACP.

Note: The LACP module can have a maximum of four groups, and up to eight ports can be in a LAG (Link Aggregation Group) at any time.

These S3280 commands provide Link Aggregation Control Protocol (LACP) functions.

>**lcp ?**

Available Commands:

LACP Configuration [<port_list>
LACP Mode [<port_list>] [enable|disable]
LACP Key [<port_list>] [<key>]
LACP Prio [<port_list>] [<prio>]
LACP System Prio [<sysprio>]
LACP Role [<port_list>] [active|passive]
LACP Status [<port_list>]
LACP Statistics [<port_list>] [clear]
LACP Timeout [<port_list>] [fast|slow]

The S3280 Link Aggregation (Aggr) commands are explained below.

Command: Display Current LACP Config

Syntax: `lACP config [<port_list>]`

Description: Displays the current LACP configuration in terms of each port's Mode, Key, and Role, where: `<port_list>`: Port list or 'All'. The default is 'All' ports.

Example: `>lACP config`

```
LACP Configuration:
=====

Port  Mode      Key  Role
----  -
1     Enabled    2    Active
2     Disabled   Auto Active
3     Disabled   Auto Active
4     Disabled   Auto Active
5     Disabled   Auto Active
6     Disabled   Auto Active
7     Disabled   Auto Active
8     Enabled    Auto Active
>
```

Command: Set / Show LACP Mode

Syntax: `lACP mode [<port_list>] [enable|disable]`

Description: Set or show LACP mode. 'LACP Enabled' controls whether LACP is enabled on this S3280 port. LACP will form an aggregation when 2 or more ports are connected to the same partner. LACP can form up to 12 LLAGs per S3280, where: `<port_list>`: Port list or 'all', default: All ports. The port specified can not already be included in a static aggregation.
enable : Enable LACP protocol.
disable: Disable LACP protocol.
(The default is 'Show LACP mode'.)

Example: `LACP>mode 8,9 enable`

`LACP>mode`

```
Port  Mode
----  -
1     Enabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Enabled
LACP>
```

Messages: *Can not enable LACP on port 5 because it already has 802.1X enabled.
Port x is already included in a static aggregation*

Command: Set / Show LACP Key**Syntax:** **lACP key** [<port_list>] [<key>]

Description: Set or show the LACP key. The Key value incurred by the port, range 1-65535. The Auto setting will set the key as appropriate by the physical link speed (10Mb = 1, 100Mb = 2, 1Gb = 3). Using the 'Specific' setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot. The LACP Key parameters are:
 <port_list>: Port list or 'All'. The default is 'All ports'.
 <key> : LACP key (1-65535) or 'Auto'. The default is 'Auto'.

Example: LACP>**key 1 1**
 LACP>**key**

```

Port  Key
----  ----
1      1
2      Auto
3      Auto
4      Auto
5      Auto
6      Auto
7      Auto
8      Auto
LACP>

```

Messages: *Can not enable LACP on port 2 because it already has 802.1X enabled.
 Port x is already included in a static aggregation*

Command: Set / Show LACP Role**Syntax:** **lACP role** [<port_list>] [active|passive]

Description: Sets or displays the LACP Role. The Role sets the LACP activity status. Enter 'Active' to transmit LACP packets each second, or enter 'Passive' to wait for a LACP packet from a partner (i.e., 'speak only if spoken to'). The LACP Role parameters are:
 <port_list>: Port list or 'All'. The default is 'All' ports.
active : Initiate LACP negotiation.
passive: Listen for LACP packets.
 (The default is 'Show LACP role'.)

Example: LACP>**role 1 passive**
 LACP>**role 2 passive**
 Port 2 is already included in a static aggregation
 LACP>**role**

```

Port  Role
----  -----
1      Passive
2      Active
3      Active
4      Active
5      Active
6      Active
7      Active
8      Active
LACP>

```

Messages: *Port x is already included in a static aggregation*

Command: Show Current LACP Status

Syntax: `lACP status [<port_list>]`

Description: Displays the current LACP Status in terms of each port's Key, Aggr ID, Partner System ID and Partner Port.

Example: LACP>`status`

Port	Mode	Key	Aggr ID	Partner System ID	Partner Port
1	Disabled	1	-	-	-
2	Disabled	1	-	-	-
3	Disabled	1	-	-	-
4	Disabled	2	-	-	-
5	Disabled	1	-	-	-
6	Disabled	1	-	-	-
7	Disabled	1	-	-	-
8	Disabled	1	-	-	-

LACP>

Command: Show / Clear LACP Statistics

Syntax: `lACP statistics [<port_list>] [clear]`

Description: Displays or clears the LACP port statistics.

Example: LACP>`statistics`

Port	Rx Frames	Tx Frames	Rx Unknown	Rx Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0

LACP>

Command: LACP Timeout

Syntax: lacp timeout [<port_list>] [fast|slow]

Description: Set or show the LACP timeout speed, where:
 <port_list>: Port list or 'All'. The default is 'All ports'.
fast : Fast PDU transmissions (fast timeout).
slow : Slow PDU transmissions (slow timeout).
 (The default is 'Show LACP timeout'.)

Example:

```
>lacp timeout
Port  Timeout
----  -
1     Fast
2     Fast
3     Fast
4     Fast
5     Fast
6     Fast
7     Fast
8     Fast
>lacp timeout 3-6 slow
>lacp timeout
Port  Timeout
----  -
1     Fast
2     Fast
3     Slow
4     Slow
5     Slow
6     Slow
7     Fast
8     Fast
>
```

Command: LACP System Prio

Syntax: lacp system prio [<sysprio>]

Description: Set or show the LACP System priority, where:
 <sysprio>: LACP System Priority setting (0-65535). The default is 32768.

Example:

```
>lacp sys prio
System Priority: 32768
>lacp sys prio 55678
>lacp sys prio
System Priority: 55678
>
```

Command: LACP Prio

Syntax: `lACP prio [<port_list>] [<prio>]`

Description: Set or show the LACP priority, where:
<port_list>: Port list or 'All'. The default is 'All ports'.
<prio> : LACP Prio (0-65535). The default is 32768.

Example:

```
>lACP prio
Port  Priority
----  -
1     32768
2     32768
3     32768
4     32768
5     32768
6     32768
7     32768
8     32768
>lACP prio 3-5 56000
>lACP prio
Port  Priority
----  -
1     32768
2     32768
3     56000
4     56000
5     56000
6     32768
7     32768
8     32768
>
```


LLDP Commands

The Link Layer Discovery Protocol (LLDP) is the IEEE 802.1ab standard specified that allows stations attached to an IEEE 802 LAN to advertise (to other stations attached to the same IEEE 802 LAN) the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

The S3280 commands provide Link Layer Discovery Protocol (LLDP) functions. The available LLDP commands are listed below.

>**lldp ?**

Available Commands:

LLDP Configuration [<port_list>]

LLDP Mode [<port_list>] [enable|disable|rx|tx]

LLDP Optional_TLV [<port_list>] [port_descr|sys_name|sys_descr|sys_capa|mgmt_addr] [enable|disable]

LLDP Interval [<interval>]

LLDP Hold [<hold>]

LLDP Delay [<delay>]

LLDP Reinit [<reinit>]

LLDP Statistics [<port_list>] [clear]

LLDP Info [<port_list>]

LLDP cdp_aware [<port_list>] [enable|disable]

>

The S3280 LLDP commands are explained below.

Command: **LLDP Configuration**

Syntax: **lldp configuration** [<port_list>]

Description: Displays the current LLDP configuration, where:
 <port_list>: Port list or 'all', default: All ports.

Example:

```
>lldp config
```

```
LLDP Configuration:
```

```
=====
```

```
Interval      : 30
Hold          : 3
Tx Delay      : 2
Reinit Delay: 2
```

Port	Mode	Port Descr	System Name	System Descr	System Capa	Mgmt Addr	CDP awareness
1	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled
2	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled
3	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled
4	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled
5	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled
6	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled
7	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled
8	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled

```
>
```

Command: Set / Show LLDP Mode

Syntax: `lldp mode [<port_list>] [enable|disable|rx|tx]`

Description: Set or show LLDP mode, where:

<port_list>: Port list or 'all', default: All ports.

enable : Enable LLDP reception and transmission. The switch will send out LLDP information, and will analyze LLDP information received from neighbours.

disable: Disable LLDP. The switch will not send out LLDP information, and will drop LLDP information received from neighbours.

rx : Enable LLDP reception only. The S3280 will not send out LLDP information, but LLDP information from neighbour units is analyzed.

tx : Enable LLDP transmission only. The switch will drop LLDP information received from neighbours, but will send out LLDP information.

(The default is 'Show LLDP mode'.)

Example: `>lldp mode 3,4,5 tx`
`>lldp mode`

```
Port  Mode
-----
1     Disabled
2     Disabled
3     Tx
4     Tx
5     Tx
6     Disabled
7     Disabled
8     Disabled
>
```

Command: **Set / Show LLDP Optional_TLV**

Syntax: **lldp optional_tlv** [<port_list>] [port_descr|sys_name|sys_descr|sys_capa|mgmt_addr] [enable|disable]

Description: An LLDP frame contains multiple TLVs (Type Length Values). An LLDP frame can contain multiple pieces of information. Each of these pieces of information is a 'TLV'. For some TLVs it is configurable if the S3280 includes the TLV in the LLDP frame. These TLVs are known as 'optional TLVs'. If an optional TLV is disabled the corresponding information is not included in the LLDP frame. This command lets you set or show LLDP Optional TLVs, where:

<port_list>: Port list or 'all', default: All ports.

port_descr : Description of the port to be included in LLDP information transmitted.

sysm_name : System name to be included in LLDP information transmitted.

sys_descr : Description of the system to be included in LLDP information transmitted.

sys_capa : System capabilities to be included in LLDP information transmitted.

mgmt_addr : Master's IP address to be included in LLDP information transmitted.

(default: Show optional TLV's configuration)

enable : Enables TLV.

disable : Disable TLV.

(default: Show optional TLV's configuration)

Example:

```
>lldp Optional_TLV all sys1 engsys1 opttlvenabl 192.168.1.110 enable
Invalid parameter: sys1
>lldp optional_tlv
```

Port	Port Descr	System Name	System Descr	System Capa	Mgmt Addr
1	Enabled	Enabled	Enabled	Enabled	Enabled
2	Enabled	Enabled	Enabled	Enabled	Enabled
3	Enabled	Enabled	Enabled	Enabled	Enabled
4	Enabled	Enabled	Enabled	Enabled	Enabled
5	Enabled	Enabled	Enabled	Enabled	Enabled
6	Enabled	Enabled	Enabled	Enabled	Enabled
7	Enabled	Enabled	Enabled	Enabled	Enabled
8	Enabled	Enabled	Enabled	Enabled	Enabled

>

Command: **Set / Show LLDP Interval**

Syntax: **lldp interval** [<interval>]

Description: Set or show LLDP Tx interval. The switch periodically transmits LLDP frames to its neighbours for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are 5 - 32768 seconds. The default is 30 seconds.

Example:

```
>lldp interval 9
>lldp interval
Interval      : 9
>
```

Command: Set / Show LLDP Hold

Syntax: **lldp hold** [<hold>]

Description: Set or show LLDP Tx hold value. Each LLDP frame contains information about how long the information in the LLDP frame is considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are 2 - 10 times. The default is 4 times.

Example:

```
>lldp hold 5
>lldp hold
Hold           : 5
>
```

Command: Set / Show LLDP Delay

Syntax: **lldp delay** [<delay>]

Description: Set or show LLDP Tx delay. If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. The 'Tx Delay' cannot be larger than 1/4 of the 'Tx Interval' value. Valid values are 1 - 8192 seconds. The default is 2 seconds.

Example:

```
>lldp delay 11
Delay must be less than 1/4 of Interval
>lldp delay 1
>lldp delay
Tx Delay      : 1
>
```

Command: Set / Show LLDP Reinit Delay

Syntax: **lldp reinit** [<reinit>]

Description: Set or show LLDP reinitialization delay. When a port is disabled, LLDP is disabled or the S3280 is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. The 'Tx Reinit' value defines the number of seconds between the shutdown frame and a new LLDP initialization. Valid values are 1 - 10 seconds. The default is 2 seconds.

Example:

```
>lldp reinit 1
>lldp reinit
Reinit Delay: 1
>
```

Command: Display / Clear LLDP Statistics

Syntax: `lldp statistics` [<port_list>] [clear]

Description: Displays or clears the current LLDP counters data for one or more S3280 ports.

Example:

```
>lldp statistics
```

```
LLDP global counters
```

```
Neighbor entries was last changed at 1970-01-01T04:15:17+00:00 (466 sec. ago).
```

```
Total Neighbors Entries Added 3.
```

```
Total Neighbors Entries Deleted 2.
```

```
Total Neighbors Entries Dropped 0.
```

```
Total Neighbors Entries Aged Out 0.
```

```
LLDP local counters
```

Port	Rx Frames	Tx Frames	Rx Errors	Rx Discards	Rx TLV Errors	Rx TLV Unknown	Rx TLV Organiz.	Aged
1	0	373	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	526	529	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

```
>lldp statistics clear
```

```
>lldp statistics
```

```
LLDP global counters
```

```
Neighbor entries was last changed at 1970-01-01T04:23:50+00:00 (2 sec. ago).
```

```
Total Neighbors Entries Added 0.
```

```
Total Neighbors Entries Deleted 0.
```

```
Total Neighbors Entries Dropped 0.
```

```
Total Neighbors Entries Aged Out 0.
```

```
LLDP local counters
```

Port	Rx Frames	Tx Frames	Rx Errors	Rx Discards	Rx TLV Errors	Rx TLV Unknown	Rx TLV Organiz.	Aged
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

```
>
```

Command: **Display Current LLDP Info**

Syntax: **lldp info** [<port_list>]

Description: Displays existing (configured) LLDP neighbor device information, where:
<port_list>: Port list or 'All'. The default is 'All' ports.

Example:

```
>lldp info

Local port           : Port 5
Chassis ID          : 00-C0-F2-00-00-01
Port ID             : 1001
Port Description    : Port #1
System Name         :
System Description  : S3280 (standalone) 1.1.6 2012-03-02T12:24:49-0 6:00
System Capabilities : Bridge(+)
Management Address  : 192.168.1.10 (IPv4)

>
```

Messages: *No LLDP entries found* displays if no LLDP neighbor exists.

Command: Set / Show LLDP CDP Aware

Syntax: `lldp cdp_aware` [<port_list>] [enable|disable]

Description: Set or show if discovery information from received CDP (Cisco® Discovery Protocol) frames is added to the LLDP neighbor table. The parameters are:

<port_list>: Port list or 'all'. The default is 'All' ports.

enable : Enable CDP awareness (CDP discovery data added to the LLDP neighbor table).

disable: Disable CDP awareness.

(The default is 'Show CDP awareness configuration'.)

```

Example: >lldp cdp_aware

Port  CDP awareness
----  -
1     Disabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
>lldp cdp_aware 2-5 enable
>lldp cdp_aware

Port  CDP awareness
----  -
1     Disabled
2     Enabled
3     Enabled
4     Enabled
5     Enabled
6     Disabled
7     Disabled
8     Disabled
>

```

The CDP operation is restricted to decoding incoming CDP frames (the S3280 does not transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled.

Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbours' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbours' table as follows:

CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.

CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbours table.

CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.

CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.

Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbours' table.

If all ports have CDP awareness disabled, the S3280 forwards CDP frames received from neighbour devices. If at least one S3280 port has CDP awareness enabled, then all CDP frames are terminated by the S3280.

Note: When CDP awareness on a port is disabled, the CDP information is not removed immediately, but gets removed when the hold time is exceeded.

Thermal Commands

These commands let you inspect and configure the current setting for controlling thermal protection. Thermal protection is used to protect the S3280 chip from getting overheated.

When the temperature exceeds the configured thermal protection temperature, ports will be turned off in order to decrease the power consumption. It is possible to arrange the ports with different priorities. Each priority can be given a temperature at which the corresponding ports will be turned off.

These S3280 commands provide Thermal protection functions.

>**thermal ?**

Available Commands:

Thermal prio_temp [<prio_list>] [<shut_down_temp>]

Thermal port_prio [<port_list>] [<prio>]

Thermal status

Thermal configuration

>

The S3280 Thermal protection commands are explained below.

Command: **Set / Show Thermal prio_temp**

Syntax: **thermal prio_temp** [<prio_list>] [<shut_down_temp>]

Description: Temperature settings for priority groups - the temperature at which the ports with the corresponding priority will be turned off. Temperatures between 0 and 255 C are supported. Set or show the temperature at which the ports will be shut down, where:

<prio_list> : List of priorities (0-3).

<shut_down_temp>: The temperature at which ports will be shut down (0-255 degrees C).

Example: >**thermal prio_temp 0 250**
 >**thermal prio_temp 1 251**
 >**thermal prio_temp 2 252**
 >**thermal prio_temp 3 253**
 >**thermal prio_temp**

```
Priority  Temp.
-----  -
```

0	250 C
1	251 C
2	252 C
3	253 C

>

Command: Set / Show Thermal port_prio

Syntax: thermal port_prio [<port_list>] [<prio>]

Description: Set or show the ports priority. Port priorities - the priority the port belongs to. Four priority levels are supported, where:

<port_list>: Port list or 'All'. The default is 'All' ports.

<prio> : Priority (0-3)

Example:

```
>thermal port_prio 1 1
>thermal port_prio 2 2
>thermal port_prio 3 3
>thermal port_prio
```

```
Port  Prio.
----  -
1     1
2     2
3     3
4     0
5     0
6     0
7     0
8     0
>
```

Command: Show Current Thermal Status

Syntax: thermal status

Description: Displays the S3280 chip temperature in degrees Celsius and the port status (normal or fail) information.

Example:

```
>thermal status
```

```
Port  Chip Temp.  Port Status
----  -
1     65 C        Port link operating normally
2     66 C        Port link operating normally
3     65 C        Port link operating normally
4     65 C        Port link operating normally
5     66 C        Port link operating normally
6     65 C        Port link operating normally
7     65 C        Port link operating normally
8     65 C        Port link operating normally
>
```

Command: Show Current Thermal configuration
Syntax: thermal configuration
Description: Display the current thermal protection configuration.
Example: >thermal config

```
Thermal Protection Configuration:  
=====
```

```
Priority  Temp.  
-----  -  
0         250 C  
1         251 C  
2         252 C  
3         253 C
```

```
Port  Prio.  
----  -  
1     1  
2     2  
3     3  
4     0  
5     0  
6     0  
7     0  
8     0  
>
```

EVC Commands

The S3280 EVC (Ethernet Virtual Connection) commands let you configure S3280 Ethernet services in terms of EVCs and ECEs (EVC Control Entries). Only Provider Bridge based EVCs are supported on the S3280.

The EVC is an association of two or more UNIs that limits the exchange of frames to UNIs in the Ethernet Virtual Connection. The User Network Interface (UNI) is the physical interface or port that is the demarcation between the customer and the service provider/Cable Operator/Carrier/MSO. The UNI is the physical demarcation point between the responsibility of the Service Provider and the responsibility of the Subscriber.

ECEs (EVC Control Entries): Unique ECE IDs are automatically assigned to ECEs added. The possible range is from 1 through 128. The ECE ID identifies the ECE.

Ethernet Services: Generally refers to Metro Ethernet Services available from service providers (SPs) per MEF specifications (MEF 6, Ethernet Services Definitions, and MEF 10, Ethernet Services Attributes).

EVC (Ethernet Virtual Connection): An association of two or more UNIs that limits the exchange of frames to UNIs in the EVC. Generally, an EVC allows Ethernet service frames to be exchanged between UNIs that are connected via the same EVC.

Note: You must set up an EVC before trying to set up a related ECE. The set of EVC commands include:

>evc ?

Available Commands:

```

EVC Configuration [<port_list>] [<policer_id>]
EVC Port DEI [<port_list>] [<dei_mode>]
EVC Port Tag [<port_list>] [<tag_mode>]
EVC Port Addr [<port_list>] [<addr_mode>]
EVC Port L2CP [<port_list>] [<l2cp_list>] [<mode>]
EVC Policer [<policer_id>] [enable|disable] [<policer_mode>] [<cir>] [<cbs>] [<eir>] [<ebs>]
EVC Add <evc_id> [<vid>] [<ivid>] [<nni_list>] [<learning>][inner] [<it_type>] [<it_vid_mode>] [<it_vid>]
    [<it_preserve>] [<it_pcp>] [<it_dei>] [outer] [<ot_vid>]
EVC Delete <evc_id>
EVC Lookup [<evc_id>]
EVC Status [<evc_id>]
EVC Statistics [<port_list>] [<class_list>] [<command>]
EVC ECE Add [<ece_id>] [<ece_id_next>] [uni] [<uni_list>]
    [<dmac_type>] [<smac>]
    [tag] [<tag_type>] [<vid>] [<pcp>] [<dei>]
    [all |
    (ipv4 [<proto>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) |
    (ipv6 [<proto>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])]
    [direction] [<direction>]
    [evc] [<evc_id>]
    [pop] [<pop>]
    [policy] [<policy>]
    [class] [<class>]
    [outer] [<ot_mode>] [<ot_preserve>] [<ot_pcp>] [<ot_dei>]
EVC ECE Delete <ece_id>
EVC ECE Lookup [<ece_id>]
EVC ECE Status [<ece_id>]
>

```

The S3280 EVC commands are explained below.

Command: Show Current EVC Configuration

Syntax: `evc configuration [<port_list>] [<policer_id>]`

Description: Displays the current EVC configuration, where:
 <port_list> : Port list or 'All'. The default is 'All' ports (status for all 128 policers display).
 <policer_id>: Policer ID (1-128).

Example 1: `>evc config 1,2,3 3`

```

Port   DEI Mode   Tag Mode   Address
-----
1      Fixed      Outer      SMAC/SIP
2      Fixed      Outer      SMAC/SIP
3      Fixed      Outer      SMAC/SIP

Policer  State      Mode      CIR      CBS      EIR      EBS
-----
3        Disabled  Aware     0        0        0        0
>

```

Example 2:

`>evc config 1,2,3 3`

```

Port   DEI Mode   Tag Mode   Address
-----
1      Fixed      Outer      SMAC/SIP
2      Fixed      Outer      SMAC/SIP
3      Fixed      Outer      SMAC/SIP

Policer  State      Mode      CIR      CBS      EIR      EBS
-----
3        Disabled  Aware     0        0        0        0

EVC ID  VID   IVID  Learning  NNI Ports  Inner Type/Mode/VID  Inner PCP/DEI  Outer VID
-----
10      1     1     Disabled  2          None/Normal/1   Fixed 0/0  0

ECE ID  Direction  EVC ID  Tag Type  VID      PCP  DEI  Frame  UNI Ports
-----
1       Both      1       Any      Any      Any  Any  Any    1
>

```

Command: Set / Show EVC Port DEI

Syntax: `evc port dei [<port_list>] [<dei_mode>]`

Description: Set or show the port DEI mode, where:

<port_list>: Port list or 'all'. The default is 'All' ports.

<dei_mode> : DEI mode: **coloured** or **fixed**. The DEI (Drop Eligible Indicator) is a 1-bit field in the VLAN tag. The DEI mode for an NNI port determines whether frames that are transmitted on the port will have the DEI field in the outer tag marked based on the colour of the frame. The valid values are:

Coloured: The DEI is 1 for yellow frames and 0 for green frames.

Fixed: The DEI value is determined by ECE rules. The default is 'Fixed'.

```
Example: >evc port dei 1,2,3 coloured
>evc port dei
Port   DEI Mode
----  -
1      Coloured
2      Coloured
3      Coloured
4      Fixed
5      Fixed
6      Fixed
7      Fixed
8      Fixed
>
```

Command: Set / Show EVC Port Tag

Syntax: `evc port tag [<port_list>] [<tag_mode>]`

Description: Set or show the port tag match mode, where:

<port_list>: Port list or 'all'. The default is 'All' ports.

<tag_mode> : Tag mode: inner or outer tagging mode. The default is 'Outer'.

```
Example: >evc port tag 1,2,3 inner
>evc port tag 4,5,6,7,8,9 outer
>evc port tag
Port   Tag Mode
----  -
1      Inner
2      Inner
3      Inner
4      Outer
5      Outer
6      Outer
7      Outer
8      Outer
>
```

Command: Set / Show EVC Port Addr

Syntax: `evc port addr [<port_list>] [<addr_mode>]`

Description: Set or show port address match mode. 'DMAC/DIP' indicates Destination MAC address / Destination MAC IP address. 'SMAC/SIP' indicates Source MAC address / Source MAC IP address. The parameters are:

<port_list>: Port list or 'All'. The default is 'All' ports.

<addr_mode>: IP/MAC address mode, either **source** (SMAC/SIP) or **destination** (DMAC/DIP). The default is **source** (SMAC/SIP) for each port.

Example: `>evc port addr 1,2,3 destination`

```
>evc port addr
```

```
Port  Address
```

```
-----
```

```
1      DMAC/DIP
```

```
2      DMAC/DIP
```

```
3      DMAC/DIP
```

```
4      SMAC/SIP
```

```
5      SMAC/SIP
```

```
6      SMAC/SIP
```

```
7      SMAC/SIP
```

```
8      SMAC/SIP
```

```
>
```

Command: Set / Show EVC Port L2CP

Syntax: `evc port l2cp [<port_list>] [<l2cp_list>] [<mode>]`

Description: Set or show port L2CP mode. L2CP Handling, per MEF 6, defines the processing of a customer’s Layer 2 Control Protocol (L2CP) frames on a given UNI for EPL and EVPL service definitions. L2CP handling requirements are specified by protocol, telling which protocols to tunnel and which to discard. See <http://metroethernetforum.org/PDFs/Standards/mef6.doc>. **Note** that you can use the “Set / Show EVC Port L2CP” CLI command, but not the S3280 web interface, to configure or display the L2CP settings. See the S3280 User Guide for more information on the web interface. See the L2CP IEEE standards at <http://standards.ieee.org/develop/regauth/grpmac/public.html>. The parameters are:

<port_list>: Port list or 'all'. The default is ‘All’ ports.

<l2cp_list>: L2CP ID list (0-31). BPDU range: 0-15, GARP range: 16-31.

BPDU range: 0-15

ID 0 reference 01-80-C2-00-00-00

ID 1 reference 01-80-C2-00-00-01

.... :..... :..

ID 12 reference 01-80-C2-00-00-0F

ID 15 reference 01-80-C2-00-00-0F

GARP range: 16-31

ID 16 reference 01-80-C2-00-00-20

ID 17 reference 01-80-C2-00-00-21

.... :..... :..

ID 31 reference 01-80-C2-00-00-2F

See the [L2CP IEEE standards](#).

<mode> : The mode takes one of the following values:

T (tunnel) : Forwarding of L2CP frames (GARP default).

P (peerDiscard) : Peers if the protocol is enabled, else discards (BPDU default).

Example 1:

```
>evc port l2cp
Port  BPDU  GARP
-----
1      P P P P P P P P-P P P P P P P P P-P T T T T T T T T-T T T T T T T T
2      P P P P P P P P-P P P P P P P P P-P T T T T T T T T-T T T T T T T T
3      P P P P P P P P-P P P P P P P P P-P T T T T T T T T-T T T T T T T T
4      P P P P P P P P-P P P P P P P P P-P T T T T T T T T-T T T T T T T T
5      P P P P P P P P-P P P P P P P P P-P T T T T T T T T-T T T T T T T T
6      P P P P P P P P-P P P P P P P P P-P T T T T T T T T-T T T T T T T T
7      P P P P P P P P-P P P P P P P P P-P T T T T T T T T-T T T T T T T T
8      P P P P P P P P-P P P P P P P P P-P T T T T T T T T-T T T T T T T T
>evc port l2cp 2-4 16 t
>evc port l2cp 2-4 16
Port  BPDU  GARP
-----
2      P P P P P P P P-P P P P P P P P P-P T T T T T T T T-T T T T T T T T
3      P P P P P P P P-P P P P P P P P P-P T T T T T T T T-T T T T T T T T
4      P P P P P P P P-P P P P P P P P P-P T T T T T T T T-T T T T T T T T
>
```

The L2CP settings do not map exactly as the MEF defines; the table below shows the S3280 L2CP behavior. There is no explicit way to 'discard', but only to redirect to CPU and if no protocol is instantiated on that port, then it is discarded. The BPDU/GARP behavior works a little different under normal mode as well (more to the IEEE recommendation).

The L2CP MIB is based on the MEF-UNI MIB. Use the table below to decode the S3280 L2CP settings.

L2CP	<u>N</u>ormal	<u>R</u>edirect	<u>F</u>orward
BPDU	Discards (or Peers, depending on if the protocol is enabled on that port)	Peers (or discards depending on if the protocol is enabled on that port)	Tunnel
GARP	Tunnel	Discards (since GARP protocols are not supported)	Tunnel

At software version 1.2.3, the L2CP default changed from 'Normal' to (BPDU -> Peer, GARP -> tunnel) for both the S3280 CLI and SNMP.

Command: Set / Show EVC Policer**Syntax:** **evc policer** [<policer_id>][enable|disable][<policer_mode>][<cir>][<cbs>][<eir>][<ebs>]**Description:** Set or show EVC bandwidth profile, where:

<policer_id> : The Policer ID (1-128).

enable : Enable EVC policer.**disable** : Disable EVC policer.

<policer_mode>: The colour mode of the bandwidth profile. The valid values are:

Coupled: Colour-aware mode with coupling enabled.**Aware**: Colour-aware mode with coupling disabled.

<cir> : Committed Information Rate [kbps] of the BWP. The valid range is 0 - 10000000 kilobits per second.

<cbs> : Committed Burst Size [bytes] of the BWP. The valid range is 0 - 100000 bytes.

<eir> : Excess Information Rate [kbps] of the BWP. The valid range is 0 - 10000000 kilobits per second.

<ebs> : Excess Burst Size [bytes] of the BWP. The valid range is 0 - 100000 bytes.

Example:

```

>evc policer 1
Policer State      Mode      CIR      CBS      EIR      EBS
-----
1      Disabled  Aware    0         0         0         0
>evc policer 1 enable coupled 1 1 1 1
>evc policer 1
Policer State      Mode      CIR      CBS      EIR      EBS
-----
1      Enabled   Coupled  1         1         1         1
>evc policer 2 enable coupled 2 3 4 5
>evc policer 2
Policer State      Mode      CIR      CBS      EIR      EBS
-----
2      Enabled   Coupled  2         3         4         5
>evc policer 3 99999 99999 99999 99999
>evc policer 3
Policer State      Mode      CIR      CBS      EIR      EBS
-----
3      Enabled   Aware    99999    99999    99999    99999
>

```

CIR is the average bit rate of Ethernet service frames (does not include the preamble, start of frame delimiter, or inter-frame gap). CIR defines the average bandwidth that the service provider guarantees the user, regardless of network conditions. CIR is typically provided incrementally, and it must be less than or equal to the UNI rate.

CBS is the maximum number of bytes allowed for a burst of back-to-back Ethernet frames. If a frame size exceeds the CBS, the frame will be either buffered or discarded (see EBS).

EIR is an average rate of Ethernet frames allowed into the network based on a “best effort” basis. Service performance for these frames is not guaranteed and depends on available bandwidth. The combined CIR and EIR must not exceed the UNI rate.

EBS helps control congestion by allowing user traffic to briefly exceed the CBS threshold and still remain within service boundaries. EBS frames are permitted into the network without performance guarantees and may be queued if bandwidth is not available. Ethernet frames exceeding the EBS threshold are discarded (frames exceeding the CBS if EBS is set to zero are also discarded).

Command: Add / Modify EVC

Syntax: **evc add** <evc_id> [<vid>] [<ivid>] [<nni_list>] [<learning>] [inner] [<it_type>] [<it_vid_mode>] [<it_vid>] [<it_preserve>] [<it_pcp>] [<it_dei>] [outer] [<ot_vid>]

Description: Add a new or modify an existing EVC, where:

<evc_id> : The EVC ID (1-128 or **none**) that identifies the EVC.

<vid> : EVC VLAN ID. The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLAN configuration. The valid range is 1 - 4094.

<ivid> : Internal VLAN ID.

<nni_list> : NNI port list (1-9) or 'none'

<learning> : Learning mode: **enable|disable**. The learning mode for the EVC controls whether source MAC addresses are learned for frames matching the EVC. Learning may be disabled if the EVC only includes two UNI/NNI ports.

The valid values are:

Enabled: Learning is enabled (MAC addresses are learned).

Disabled: Learning is disabled (MAC addresses are not learned).

inner : Inner tag action keyword

<it_type> : Inner tag type: **none|c-tag|s-tag|s-custom-tag**.

<it_vid_mode>: Inner VID mode: **normal|tunnel**

<it_vid> : Inner tag VLAN ID (1-4094).

<it_preserve>: Inner tag preserved or fixed PCP/DEI; either **preserve** or **fix**.

<it_pcp> : Inner tag PCP value (0-7).

<it_dei> : Inner tag DEI value (0-1).

outer : Outer tag action keyword.

<ot_vid> : EVC outer tag VID for UNI ports.

Note: when done, use the **EVC Lookup** command to verify the new EVC's configuration.

Example 1:

```
>evc add 1 1 1 1 enable I C Tunnel 1 preserve 0 0 0 1
>evc add 2 1 1 1 enable I S-tag Tunnel 1 preserve 0 0 0 2
>evc lookup 2
```

EVC ID	VID	IVID	Learning	NNI Ports	Inner Type/Mode/VID	Inner PCP/DEI	Outer VID
2	1	1	Enabled	1	S/Tunnel/1	Pres. 0/0	2

```
>evc lookup 1
```

EVC ID	VID	IVID	Learning	NNI Ports	Inner Type/Mode/VID	Inner PCP/DEI	Outer VID
1	1	1	Enabled	1	C/Tunnel/1	Pres. 0/0	1

Example 2:

```
>evc look
```

EVC ID	VID	IVID	Learning	NNI Ports	Inner Type/Mode/VID	Inner PCP/DEI	Outer VID
1	100	1	Enabled	4-6	C/Normal/100	Fixed 0/0	100

Messages: *EVC 1 does not exist*

Command: Delete Existing EVC

Syntax: `evc delete <evc_id>`

Description: Delete an existing EVC, where:
 <evc_id>: an existing EVC ID (1-128).

Example:

```
>evc delete 2
>evc lookup
```

EVC ID	VID	IVID	Learning	NNI Ports	Inner Type/Mode/VID	Inner PCP/DEI	Outer VID
1	1	1	Enabled	1	C/Tunnel/1	Pres. 0/0	1

```
>
>evc lookup 2
EVC 2 does not exist
>
```

Note: when done, use the **EVC Lookup** command to verify that the EVC was deleted.

Command: EVC Status

Syntax: `evc status [<evc_id>]`

Description: Show the current EVC Status, where:
 <evc_id>: An existing EVC ID (1-128).

Example 1:

```
>evc status
```

EVC ID	VID	IVID	Conflict
1	1	1	No

```
>evc status 2
EVC 2 does not exist
>evc status
```

EVC ID	VID	IVID	Conflict
10	1	1	No

```
>
```

Example 2:

```
>evc status
```

EVC ID	VID	IVID	Conflict
1	1	1	No
2	1	1	No

```
>
```

Command: EVC Lookup

Syntax: `evc lookup [<evc_id>]`

Description: Lookup one or more EVCs, where
 <evc_id>: An existing EVC ID (1-128). If the EVC has not been added, the message “EVC x does not exist” displays. Verify the <evc_id> parameter in this case.

Example 1:

```
>evc lookup 1
EVC ID  VID  IVID  Learning  NNI Ports  Inner
-----  ----  ----  -
1         1     1     Enabled   1          C/Tunnel/1  Inner
                                     Type/Mode/VID  PCP/DEI  Outer
                                     -----  -
                                     Pres. 0/0  VID
>
```

Example 2:

```
>evc lookup 1
EVC ID  VID  IVID  Learning  NNI Ports  Inner
-----  ----  ----  -
1         1     1     Disabled  3,4       S/Normal/1  Inner
                                     Type/Mode/VID  PCP/DEI  Outer
                                     -----  -
                                     Fixed 0/0  VID
ECE ID           : 1
Key Parameters
-----
UNI Ports        : 7,8
DMAC Type        : Any
SMAC              : Any
Outer Tag Type   : Any
Outer VID        : Any
Outer PCP        : Any
Outer DEI        : Any
Frame Type       : Any
Action Parameters
-----
Direction        : Both
EVC ID           : 1
Tag Pop Count    : 0
Policy Number    : 0
Class            : Disabled
Outer Mode       : Disabled
Outer PCP/DEI    : Fixed
Outer PCP        : 0
Outer DEI        : 0
Conflict         : No
ECE ID           : 2
Key Parameters
-----
UNI Ports        : 2,7
DMAC Type        : Any
SMAC              : Any
Outer Tag Type   : Any
Outer VID        : Any
```

```
Outer PCP      : Any
Outer DEI      : Any
Frame Type     : Any
```

Action Parameters

```
Direction      : Both
EVC ID         : 1
Tag Pop Count   : 0
Policy Number   : 0
Class          : Disabled
Outer Mode      : Disabled
Outer PCP/DEI  : Fixed
Outer PCP       : 0
Outer DEI       : 0
Conflict       : No
>
```

Command: EVC Statistics**Syntax:** **evc statistics** [<port_list>] [<class_list>] [<command>]**Description:** Show or clear EVC statistics. With no qualifying parameters, the 'show' version of this command can be very long. The valid parameters are:

<port_list> : Port list or 'all'. The default is 'All' ports.

<class_list>: QoS (Quality of Service) class list, 0-7.

<command> : Statistics command: clear|green|yellow|red|discard.

clear: Erase (clear) all stored EVC statistics.**green:** Show (display) all stored RX Green and TX Green EVC statistics.**yellow:** Show (display) all stored RX Yellow and TX Yellow EVC statistics.**red:** Show (display) all stored RX Red and TX Red EVC statistics.**discard:** erase (discard) all stored EVC statistics.**Example:**

```

>evc statistics 1 7
Port 1, Priority 7 Statistics:

Rx Green:                0      Tx Green:                7351
Rx Yellow:               0      Tx Yellow:                0
Rx Red:                  0
Rx Green Discard:        0
Rx Yellow Discard:       0
>evc statistics 1 1 red
Port  Class  Rx Red
----  -
1     1      0
>evc statistics 1 1 yellow
Port  Class  Rx Yellow          Tx Yellow
----  -
1     1      0                      0
>evc statistics 1 1 green
Port  Class  Rx Green          Tx Green
----  -
1     1      0                      0
>evc statistics 1,2 1,2 discard
Port  Class  Rx Green Discard  Rx Yellow Discard
----  -
1     1      0                      0
1     2      0                      0
2     1      0                      0
2     2      0                      0
>

```

Command: Add EVC ECE

Syntax: **evc ece add** [<ece_id>] [<ece_id_next>] [uni] [<uni_list>]
 [<dmac_type>] [<smac>]
 [tag] [<tag_type>] [<vid>] [<pcp>] [<dei>]
 [all |
 (ipv4 [<proto>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) |
 (ipv6 [<proto>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])]
 [direction] [<direction>]
 [evc] [<evc_id>]
 [pop] [<pop>]
 [policy] [<policy>]
 [class] [<class>]
 [outer] [<ot_mode>] [<ot_preserve>] [<ot_pcp>] [<ot_dei>]

Description: Add or modify EVC Control Entry (ECE):

- * If <ece_id> is specified and the ECE exists, the ECE will be modified.
- * If <ece_id> is omitted or the ECE does not exist, a new ECE will be added.
- * If <ece_id_next> is specified, the ECE will be placed before this entry.
- * If <ece_id_next> is 'last', the ECE will be placed at the end of the list.
- * If <ece_id_next> is omitted and it is a new ECE, the ECE will be placed last.
- * If <ece_id_next> is omitted and the ECE exists, the ECE will not be moved.

Note: You must set up an EVC before trying to set up a related ECE.

The EVC ECE parameters are:

<ece_id> : ECE ID (1-128)

<ece_id_next>: Next ECE ID (1-128) or 'last'.

uni : UNI keyword.

<uni_list> : UNI port list (1-9).

<dmac_type> : DMAC type: any|unicast|multicast|broadcast.

<smac> : SMAC or 'any'.

tag : Tag matching keyword.

<tag_type> : Tag type: tagged|untagged|any.

<vid> : VLAN ID value/range (0-4094) or 'any'.

<pcp> : PCP value/range (0-7) or 'any'.

<dei> : DEI value, 0, 1 or 'any'.

all : Keyword for matching any frame type.

ipv4 : Keyword for matching IPv4 frames.

<proto> : IP protocol value (0-255) or 'any'.

<sip> : IPv4 source address (a.b.c.d/n) or 'any'.

<dscp> : DSCP value/range (0-63) or 'any'.

<fragment> : IPv4 fragment: any|fragment|non-fragment.

<sport> : UDP/TCP Source port value/range (0-65535) or 'any'.

<dport> : UDP/TCP Destination port value/range (0-65535) or 'any'.

ipv6 : Keyword for matching IPv6 frames.

<sip_v6> : IPv6 source address (a.b.c.d/n) or 'any'.

direction : Direction keyword.

<direction> : ECE direction: both|uni-to-nni|nni-to-uni (see Note below).

evc : EVC keyword.

<evc_id> : EVC ID (1-128) or 'none'.

pop : Pop keyword.

<pop> : Tag pop count: 0|1|2.

policy : Policy keyword.

<policy> : ACL policy number (0-255).

class : Class keyword.

<class> : QoS class, 'disable' or 0-7.
 outer : Outer tag action keyword.
 <ot_mode> : Outer tag for nni-to-uni direction: enable|disable.
 <ot_preserve>: Outer tag preserved or fixed PCP/DEI: preserved|fixed.
 <ot_pcp> : Outer tag PCP value (0-7).
 <ot_dei> : Outer tag DEI value (0-1).

Example:

```
>evc ece add 1 1 1 1 unicast any T tagged 1 1 1 A 4 1 any 1 fragment any any 6 any D nni-to-uni V 1
P 1 1 1 1 K 1 O enable fixed 1 1
>
```

Messages: Invalid parameter: unicast

Note: The EVCs and ECEs are used to set up flows in one or both directions as determined by the ECE "direction" parameter. If the ECE is bidirectional, the ingress rules of the NNI ports will be setup to match the traffic being forwarded to NNI ports. The valid values are:

Both: Bidirectional.

UNI-to-NNI: Unidirectional from UNI to NNI.

NNI-to-UNI: Unidirectional from NNI to UNI. The 'NNI-to-UNI Tag Mode' is only used when the direction is 'NNI-to-UNI'. only applies to the 'NNI-to-UNI' direction. The 'NNI-to-UNI Tag Mode' selection is disabled when the direction is not 'NNI-to-UNI'.

The 'NNI-to-UNI Tag Mode' may be used in situations where you would like to translate from C-tag to S-tag and optionally also change the VLAN ID. Frames traversing from NNI-to-UNI will pop an S-tag, and on egress from the UNI push a new C-tag with the VLAN ID from 'EVC Configuration > Outer Tag > VLAN ID'. In the other direction you should be able to do similar actions in the ECE using 'Tag Pop Count'.

Note: Two unidirectional services in each direction do not equate to a bidirectional service. Also, it is recommended to make the NNI ports as C/S-ports and to add VLAN membership entries accordingly to ensure proper operation on the EVCs.

Command: EVC ECE Delete
Syntax: **evc ece delete** <ece_id>
Description: Delete an existing ECE, where:
 <ece_id>: ECE ID (1-128)

Example: >**evc ece delete 1**
 >

Messages: *W evc 04:37:12 50/evc_mgmt_ece_del#1297: Warning: id: 1 not found
 ECE delete failed*

Command: EVC ECE Lookup
Syntax: **evc ece lookup** [<ece_id>]
Description: Look up an existing ECE, where:
 <ece_id>: An existing ECE ID (1-128).

Example 1:

```
>evc ece lookup
ECE ID  Direction  EVC ID  Tag Type  VID  PCP  DEI  Frame  UNI Ports
-----  -
1         Both         1        Any       Any  Any  Any  Any     1
>
```

Example 2:

```
>evc ece look 1
```

```
ECE ID      : 1
```

```
Key Parameters
```

```
-----
UNI Ports      : 5
DMAC Type      : Any
SMAC           : Any
Outer Tag Type : Untagged
Outer VID      : Any
Outer PCP      : Any
Outer DEI      : Any
Frame Type     : IPv4
Protocol       : 6 (TCP)
DSCP           : Any
Fragment       : Any
Source IP      : Any
Source Port    : Any
Destination Port: Any
```

```
Action Parameters
```

```
-----
Direction      : NNI-to-UNI
EVC ID         : 1
Tag Pop Count  : 1
Policy Number  : 0
Class          : 2
Outer Mode     : Enabled
Outer PCP/DEI : Fixed
Outer PCP      : 1
Outer DEI      : 0
Conflict       : No
>
```

Messages: *ECE ID not found
 Invalid parameter: 0*

Command: EVC ECE Status

Syntax: `evc ece status [<ece_id>]`

Description: Display (show) the current status of one or more existing ECEs, where:
 <ece_id>: ECE ID (1-128) to display.

Example 1:

```
>evc ece status 2
ECE ID not found
>evc ece status 1
ECE ID          : 1

Key Parameters
-----
UNI Ports       : 1
DMAC Type      : Any
SMAC           : Any
Outer Tag Type  : Any
Outer VID      : Any
Outer PCP      : Any
Outer DEI      : Any
Frame Type     : Any

Action Parameters
-----
Direction      : Both
EVC ID         : 1
Tag Pop Count   : 0
Policy Number   : 0
Class          : Disabled
Outer Mode     : Disabled
Outer PCP/DEI  : Fixed
Outer PCP      : 0
Outer DEI      : 0
Conflict       : No
>
```

Example 2:

```
>evc ece status 1
ECE ID          : 1

Key Parameters
-----
UNI Ports       : 1,2,8
DMAC Type      : Unicast
SMAC           : Any
Outer Tag Type  : Tagged
Outer VID      : Any
Outer PCP      : Any
Outer DEI      : Any
Frame Type     : IPv4
Protocol       : 6 (TCP)
DSCP           : Any
Fragment      : Fragment
Source IP      : Any
Source Port    : Any
Destination Port: Any

Action Parameters
-----
Direction      : UNI-to-NNI
EVC ID         : 1
Tag Pop Count   : 1
```

```
Policy Number : 0
Class         : 5
Outer Mode    : Enabled
Outer PCP/DEI : Preserved
Outer PCP     : 0
Outer DEI     : 1
Conflict      : No
```

Example 3:

```
>evc ece status
ECE ID  Direction  EVC ID  Conflict
-----  -
1       NNI-to-UNI  1       No
2       Both      1       No
>
```

Messages:

ECE ID not found

Invalid parameter: 0

EPS Commands

EPS (Ethernet Protection Switching) is defined in ITU/T G.8031. The S3280 implements the ITU G.8031 standard for EPS at the port level. It can perform 1:1 and 1+1 protection in unidirectional and bidirectional switching. The EPS feature provides the option to configure revertive and non-revertive mode in both 1:1 and 1+1 switching. It also allows configuring WTR (Wait To Restore) timer in revertive mode to avoid a ‘flapping’ working link which could trigger constant protection switching. A misconfigured or mismanaged router may get into a rapid cycle between down and up states. This pattern of repeating withdrawal and re-announcement is known as route ‘flapping’ and it can cause excessive activity in all the other routers that know about the broken link, as the same route is continuously injected and withdrawn from the routing tables. With BGP, traffic delivery may not function while routes are being updated.

The S3280 supports a ‘Hold-Off-Timer’ which would delay the protection switching until an upstream device or the lower layer is ready. Both the WTR and Hold-Off-Timer are configurable in fine granular time increments.

The EPS instance is associated with the MEPs on the working and protection links which are responsible for sending/receiving APS frames. The MEPs associated with the EPS must have APS enabled for protection. The APS frames can be unicast to the peer or a multicast. The APS frames can carry specific commands to its peer entity. When there is a failure in the working link in 1+1 or 1:1 switching, the protection link takes over.

These S3280 commands provide Ethernet linear Protection Switching (EPS) functions.

>eps ?

Available Commands:

EPS create [<inst>] [domport] [1p1|1f1] [<flow_w>] [<flow_p>] [<mep_w>] [<mep_p>] [<mep_aps>] [enable|disable]

EPS config [<inst>] [aps|noaps] [revert|norevert] [unidir|bidir] [w0s|w10s|w30s|w1m|w5m|w12m]
[h0s|h100ms|h500ms|h1s|h2s|h5s|h10s]

EPS command [<inst>] [clear|lockout|forced|manualp|manualw|exercise|freeze|lockoutlocal]

EPS state [<inst>]

>

The typical CLI process to create, configure, set up, and verify an EPS instance requires you to:

1. Create a new EPS instance using the **eps create** command.
2. Configure the EPS using the **eps config** command.
3. Set the EPS command operation using the **eps command** command.
4. Verify the new EPS configuration using the **eps state** command.

The S3280 EPS commands are explained below.

Command: Create EPS Instance

Syntax: **eps create** [<inst>] [domport] [1p1|1f1] [<flow_w>] [<flow_p>] [<mep_w>] [<mep_p>] [<mep_aps>] [enable|disable]

Description: Create a new EPS instance, where:

<inst> : Instance number
 domport : The Flow domain (port).
 1p1|1f1 : The EPS architecture:
 1p1: use the 1+1 EPS architecture. This will create a 1+1 EPS.
 1f1: use the 1:1 EPS architecture. The APS protocol is mandatory for 1:1 protection. This will create a 1:1 EPS.
 <flow_w> : Working flow instance number.
 <flow_p> : Protecting flow instance number.
 <mep_w> : Working MEP instance number.
 <mep_p> : Protecting MEP instance number.
 <mep_aps> : APS MEP instance number.
 enable|disable : Enable or disable EPS protection.

Example 1:

```
>eps config
```

Configuration is:

Inst	Dom	Archi	Wflow	Pflow	Wmep	Pmep	APSmep
Direct	Revert	Wtr	Hold	Aps			

```
>eps create 1 domport 1p1 1 2 3 4 5 enable
```

```
>eps config
```

Configuration is:

Inst	Dom	Archi	Wflow	Pflow	Wmep	Pmep	APSmep
Direct	Revert	Wtr	Hold	Aps			
1	Port	1plus1	1	2	3	4	5
xxx	xxx	xxx	xxx	xxx			

```
>
```

Example 2:

```
>eps create 2 domport 1f1 2 3 4 5 6 enable
```

```
>eps config
```

Configuration is:

Inst	Dom	Archi	Wflow	Pflow	Wmep	Pmep	APSmep
Direct	Revert	Wtr	Hold	Aps			
1	Port	1plus1	1	2	3	4	5
xxx	xxx	xxx	xxx	xxx			
2	Port	1for1	2	3	4	5	6
xxx	xxx	xxx	xxx	xxx			

```
>
```

Messages:

Creating an instance already created

Invalid parameter: w

Invalid parameter error returned from EPS

Invalid working SF MEP

Command: EPS Config

Syntax: **eps config** [<inst>] [aps|noaps] [revert|norevert] [unidir|bidir]
[w0s|w10s|w30s|w1m|w5m|w12m] [h0s|h100ms|h500ms|h1s|h2s|h5s|h10s]

Description: EPS config operation, where:

<inst> : Instance number
 aps|noaps : APS enable/disable
 revert|norevert : Revertive enable/disable
 unidir|bidir : Unidirectional or bidirectional switching
 w0s|w10s|w30s|w1m|w5m|w12m : Wait To Restore timer value (in seconds or minutes).
 h0s|h100ms|h500ms|h1s|h2s|h5s|h10s: Hold off timer value (in seconds or milliseconds).

Example 1:

```
>eps config 1 aps norevert bidir w10s h0s
```

Operating on an instance not created

```
>eps config
```

Configuration is:

Inst	Dom	Archi	Wflow	Pflow	Wmep	Pmep	APSmep
Direct	Revert	Wtr	Hold	Aps			
1	Port	1plus1	1	2	1	1	1
xxx	xxx	xxx	xxx	xxx			

```
>
```

Example 2:

Configuration is:

Inst	Dom	Archi	Wflow	Pflow	Wmep	Pmep	APSmep	Direct	Revert	Wtr	Hold	Aps
1	Port	1plus1	1	2	1	1	1	xxx	xxx	xxx	xxx	xxx

```
>
```

Example 3:

```
>eps config 1 aps revert bidir w10s h1s
```

```
>eps config
```

Configuration is:

Inst	Dom	Archi	Wflow	Pflow	Wmep	Pmep	APSmep
Direct	Revert	Wtr	Hold	Aps			
1	Port	1plus1	1	2	3	4	5
Bidir	True	w10s	h1s	True			
2	Port	1for1	2	3	4	5	6
xxx	xxx	xxx	xxx	xxx			

```
>
```

Messages:

EPS instance not created

Invalid parameter: w

Operating on an instance not created

Command: EPS Command

Syntax: **eps command** [<inst>] [clear|lockout|forced|manualp|manuelw|exercise|freeze|lockoutlocal]

Description: EPS command set operation. An EPS must first be created (**eps create** command above) and configured (**eps config** command above) to be able to use this command. The parameters are:
 <inst> : An existing EPS instance number.

clear|lockout|forced|manualp|manuelw|exercise|freeze|lockoutlocal: EPS protection command type, either:

none: No active local command on this instance.

clear: The active local command will be cleared.

lock Out: This EPS is locked to working (not active). In case of 1:N (more than one EPS with same protecting flow) - when one EPS switch to protecting flow, other EPS is enforced this command

forced: Forced switch to protecting.

manualp: Manual switch to protecting.

manuelw: Manual switch to working - this is only possible in 1:1 non-revertive.

exercise: Exercise of the protocol - not traffic effecting.

freeze: This EPS is locally freezed - ignoring all input.

lock out local: This EPS is locally "locked out" - ignoring local SF detected on working.

Example:

```
>eps com 1 lockoutlocal
>eps com 1 clear
>eps com 1 forced
>eps com 1 manualp
>eps com 1 exercise
>
```

Example 2:

```
>eps command 1 manualp
```

```
>eps state
```

EPS state is:

	Inst	State	Wstate	Pstate	TxAps r b	RxAps r b	Fop
Pm	FopCm	FopNr	FopNoAps				
	1	Manualp	Ok	Ok	MS 1 1	NR 0 0	Fal
se	False	True	True				
	2	Disable	Ok	Ok	NR 0 0	NR 0 0	Fal
se	False	False	False				

```
>
```

Messages: *EPS instance not created*
EPS NOT created
Operating on an instance not created

Command: Show EPS State
Syntax: eps state [<inst>]
Description: Display the current EPS protection state, where:
 <inst>: An existing Instance number.

Example:

```
>eps state

EPS state is:
Inst   State   Wstate   Pstate   TxAps r b   RxAps r b   FopPm   FopCm   FopNr   FopNoAps
2      Disable Ok        Ok        NR 0 0      NR 0 0      False   False   False   False

>
>eps state

EPS state is:
Inst   State   Wstate   Pstate   TxAps r b   RxAps r b   FopPm   FopCm   FopNr   FopNoAps
1      Forced  Ok        Ok        FS 1 1      NR 0 0      False   False   True    True

>
```

The EPS State table parameters displayed are:

Inst: An existing EPS Instance number.

State: The current EPS protection state for this instance ('enable' or 'disable').

Wstate: The current Working flow state for this instance.

Pstate: The current Protecting flow state for this instance.

TxAps r b: Transmit APS r b: The 'r b' indicates 'RPL Blocked'. This is the transmitted APS according to the State Transition Tables in the G.8032 standard.

RxAps r b: Receive APS r b: The 'r b' indicates 'RPL Blocked'. This is the transmitted APS according to the State Transition Tables in the G.8032 standard.

FopPm: Displays 'true' if a Failure of Protocol – Provisioning Mismatch has occurred, otherwise displays 'false'. Due to errors in provisioning, the ERP control process may detect a combination of conditions which should not occur during "normal" conditions. To warn the operator of such an event, a failure of protocol – provisioning mismatch (FOP-PM) is defined. The FOP-PM defect, detected if the RPL owner node receives one or more No Request R-APS message(s) with the RPL Blocked status flag set (NR, RB), and a node ID that differs from its own. The ERP control process must notify the equipment fault management process when it detects such a defect condition, and continue its operation as well as possible. This is only an overview of the defect condition. The associated defect and its details are defined in ITU-T G.8021 as amended by its Amendments 1 and 2.

FopCm: Displays 'true' if a Failure of Protocol – Configuration Mismatch has occurred, otherwise displays 'false'. Fully incompatible provisioning and working/protection Configuration mismatches are detected by receiving just one APS frame.

FopNr: The 'Nr' indicates 'No Request' (e.g., NR Null/Null displayed). No request (NR) is the ring protection condition when no local protection switching requests are active. This is the transmitted APS according to the State Transition Tables in the G.8032 standard.

FopNoAps: APS PDU not received from the other end.

When any Failure of Protocol Defect (FOP) is detected, the S3280 red LED lights; otherwise the green LED is lit.

Automatic Protection Switching (the APS protocol) is mandatory for 1:1 protection. It enables the automatic protection switching APS protocol and linear protection switching mechanisms for point-to-point VLAN-based ETH SNC in Ethernet transport networks per Rec. ITU-T G.8031/Y.1342 (11/2009).

APS protocol information transportation based on transmitting / receiving R-APS/L-APS PDU can be enabled/disabled. This must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured.

Per ITU-T Rec. G.8021/Y.1341 (2004)/Amd.1 (06/2006): provides updated material describing the functions required to support link aggregation and a subset of the Ethernet OAM, i.e., clauses 8.1 (OAM related processes), 9 (Ethernet layer functions), 9.1 (ETH_FD function), 9.2 (ETHx/ETH_A adaptation function), 9.3 (ETHG/ETH_A adaptation function), 9.5 (<server>/ETH_A adaptation function) and 9.7 (ETH link aggregation function). Amendment 1 also defines the Ethernet-specific equipment functional details for the CSF and RFI mechanisms.

Per Rec. ITU-T G.8021/Y.1341 (2007)/Amendment 2 (02/2010) – Prepublished version:

Defect Generation Process: this process detects and clears the defects (dLOC[i], dRDI[i], dLCK, dAIS, dUNL, dMMG, dUNM, dUNP, dUNPr, dDEG) as defined in Clause 6, where [i] = maintenance entity.

Defects: this function detects dLOC[i], dRDI[i], dLCK, dAIS, dUNL, dMMG, dUNM, dUNP, dUNPr, dDEG.

Defect correlations: cRDI[i] ← (dRDI[1..n]) and (MI_CC_Enable)

Performance monitoring:

pN_LFFLC ← N_LF

pN_TFC ← N_TF

pF_LFFLC ← F_LF

pF_TFNTC ← F_TF

dDEG (Degraded Signal defect) - this defect is only defined for point-to-point ETH connections. The Degraded Signal defect is calculated at the ETH layer. It monitors the connectivity of an ETH Trail. Every second the S3280 receives the 1 second counters for far near end received and transmitted frames and determines whether the second was a Bad Second. The defect is detected if there are MI_LM_DEGM consecutive Bad Seconds and cleared if there are MI_LM_M consecutive Good Seconds. In order to declare a Bad Second the number of transmitted frames must exceed a threshold (TF_MIN). If this is true then a Bad Second is declared if either the Frame Loss is negative (i.e., there are more frames received than transmitted) or the FLR (Frame Loss Ratio - lost frames/transmitted frames) is greater than MI_LM_DEGTHR.

dFOP-PM (Linear or Ring protection Failure of Protocol Provisioning Mismatch) - the Failure of Protocol Provisioning Mismatch defect is calculated at the ETH layer. It monitors provisioning mismatch of:

- Linear protection by comparing B bits of the transmitted and the received APS protocol, or
- Ring protection by comparing the Node ID of the RPL Owner and the Node ID in a received R-APS(NR, RB) frame.

dFOP-PM is detected:

- In the case of linear protection, on receipt of an APSb event and cleared on receipt of an expAPS event. These events are generated by the subnetwork connection protection process (Clause 9.1.3.), or
- In the case of ring protection, on receipt of an RAPSpm event and cleared on receipt of no RAPSpm event during K times the long R-APS frame intervals defined in G.8032/Y.1344, where $K \geq 3.5$. These events are generated by the ring protection control process (Clause 9.1.4).

Ring Protection Control Process: Ring Protection with Inherent, Sub-Layer, or Test Trail monitoring is supported. This is only an overview of the Ethernet Ring Protection Control Process as specified in ITU-T Rec. G.8032/Y.1344. The ETH_FT_Sk provides the TSF protection switching criterion via the ETH/ETH_A_Sk function (SSF). G.8032 specifies the requirements, options and the ring protection protocol supported by the ring protection control process.

The following configuration parameters are defined in G.8032/Y.1344:

ETH_C_MI_RAPS_RPL_Owner_Node configures the node type.

ETH_C_MI_RAPS_RPL_Neighbour_Node configures the adjacency of a node to the RPL Owner.

ETH_C_MI_RAPS_Propagate_TC[1...M] configures the flush logic of an interconnection node.

ETH_C_MI_RAPS-Compatible_Version configures the Backward compatibility logic.

ETH_C_MI_RAPS_Revertive configures the revertive mode.

ETH_C_MI_RAPS_Sub_Ring_Without_Virtual_Channel configures the sub-ring type.

Defects: The function detects dFOP-PM in case the R-APS protocol is used.

Defect correlations: cFOP-PM, dFOP-PM.

MEP Commands

A MEP (Maintenance Entity Endpoint) is an endpoint in a Maintenance Entity Group (per ITU-T Y.1731).

The S3280 implements Service OAM (SOAM), compliant with IEEE802.1ag and ITU Y.1731 standards. SOAM operates over the S3280 VLAN configuration.

The OAM functions are based on transmission and reception of OAM frames (i.e., PDU frames). OAM frames are exchanged within a Maintenance Entity (ME) and the points that transmit and receive OAM frames are called Maintenance Entity Group End Points (MEPs). The ME Group has a unique ID and each MEP has a unique ID within the MEG. OAM frames have a unique EtherType of 0x8902 and are transmitted either as Unicast or Multicast within a dedicated range of MAC addresses (01-80-C2-00-00-30 and 01-80-C2-00-00-3F).

ME groups can be nested but cannot overlap. To accommodate nesting, the OAM frame contains a MEG level (i.e., a MEP at a certain level will forward OAM frames of a higher level and block OAM frames at a lower level). The MEG levels are divided into three roles: the 'Customer' role is assigned three MEG levels (7, 6, and 5), the 'Provider' role is assigned two MEG levels (4 and 3), and the 'Operator' role is assigned three MEG levels (2, 1, and 0). Especially with Fault Protection, it is possible to have a MEG Intermediate Point (MIP). A MIP reacts only to link trace and Unicast Loopback PDUs, and forwards all OAM frames.

These S3280 commands provide Maintenance entity End Point (MEP) functions. **Note:** SOAM MEP configuration must be done before configuring Ethernet Ring Protection Switching.

>mep ?

Available Commands:

```

MEP config [<inst>] [mep|mip] [down|up] [<port>] [domport|domevc] [<level>] [itu|ieee] [<meg>] [<mep>] [<vid>] [<flow>]
[enable|disable]
MEP peer MEP [<inst>] [<mep>] [<mac_addr>] [enable|disable]
MEP cc config [<inst>] [<prio>] [300s|100s|10s|1s|6m|1m|6h] [enable|disable]
MEP lm config [<inst>] [<prio>] [uni|multi] [single|dual] [10s|1s|6m|1m|6h] [<flr>] [enable|disable]
MEP aps config [<inst>] [<prio>] [uni|multi] [laps|raps] [<octet>] [enable|disable]
MEP client config [<inst>] [domport|domevc] [<level>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>]
[<cflow>] [<cflow>] [<cflow>] [<cflow>]
MEP ais config [<inst>] [<prio>] [1s|1m] [set|clear] [enable|disable]
MEP lck config [<inst>] [<prio>] [1s|1m] [enable|disable]
MEP lt config [<inst>] [<prio>] [<mac_addr>] [<mep>] [<ttl>] [enable|disable]
MEP lb config [<inst>] [set|clear] [<prio>] [uni|multi] [<mac_addr>] [<mep>] [<tosend>] [<size>] [<gap>] [enable|disable]
MEP dm config [<inst>] [<prio>] [uni|multi] [<mep>] [oneway|twoway] [std|prop] [rdtrp|flow] [<gap>] [<count>] [us|ns]
[keep|reset] [d2ford1] [enable|disable]
MEP tst config [<inst>] [set|clear] [<prio>] [<mep>] [no_seq|seq] [<rate>] [<size>] [allzero|allone|onezero] [enable|disable]
MEP state [<inst>]
MEP lm state [<inst>]
MEP lm clear <inst>
MEP lt state [<inst>]
MEP lb state [<inst>]
MEP dm state [<inst>]
MEP dm clear <inst>
MEP tst state [<inst>]
MEP tst clear <inst>
>

```

The available S3280 Maintenance entity End Point (MEP) commands are explained below.

Command: MEP / MIP Instance Configuration

Syntax: **mep config** [<inst>] [mep|mip] [down|up] [<port>] [domport|domevc] [<level>] [itu|ieee] [<meg>] [<mep>] [<vid>] [<flow>] [enable|disable]

Description: Display, edit, or define a MEP instance configuration(s). For MEP instance configuration:

'mep|mip' this entity is either a MEP or a MIP - end point or intermediate point.

'down|up' this entity is either a (Ingress) down or (Egress) up type of MEP.

'domport|domevc' the domain is either Port or EVC.

'level' is the MEG level.

'port' is the residence port.

'flow' is the related flow instance number (Port # in Port domain; EVC # in EVC domain).

'vid' is used for TAGGED OAM in port domain.

'itu|ieee' is the MEG ID format.

'meg' is the MEG ID - max. 8 char in case of 'ieee' - 6 or 7 char in case of 'itu'.

'mep' is the MEP ID.

The parameters are:

<inst> : Instance number.

mep|mip : Mode of the MEP instance

down|up : Direction of the MEP instance

<port> : Port number.

domport|domevc: Flow domain

<level> : MEP level (0-7).

itu|ieee : MEG format, either:

ITU: ICC format as defined in Y.1731 ANNEX A, or

IEEE: String format Domain Name and Short Name as defined in 802.1ag.

<meg> : MEG ID (max. 8 chars)

<mep> : This MEP id (0-0x1FFF)

<vid> : C-TAG only applicable for Port MEP

<flow> : Flow instance number (Port/EVC)

enable|disable: enable/disable

Example 1:

```
>mep config
```

MEP Configuration is:

Inst	Mode	Direction	Port	Dom	Level	Format	Name	Meg id	Mep id	Vid	Flow	Eps	MAC
1	Mep	Down	1	Port	0	ITU ICC	TRNSTN	meg000	0	0	1	0	00-C0-F2-21-B8-C5
2	Mep	Down	2	Port	1	ITU ICC	TRNSTN	meg000	0	1	2	0	00-C0-F2-21-B8-C6
3	Mep	Down	3	Port	2	ITU ICC	TRNSTN	meg000	0	2	3	0	00-C0-F2-21-B8-C7
4	Mep	Down	4	Port	3	ITU ICC	TRNSTN	meg000	0	3	4	0	00-C0-F2-21-B8-C8
5	Mep	Down	5	Port	4	ITU ICC	TRNSTN	meg000	0	4	5	0	00-C0-F2-21-B8-C9

Example 2:

```
>mep config
```

MEP Configuration is:

Inst	Mode	Direction	Port	Dom	Level	Format	Name	Meg id	Mep id	Vid	Flow	Eps	MAC
1	Mep	Down	1	Port	0	ITU ICC	TRNSTN	meg000	0	0	1	0	00-C0-F2-21-B8-C5
2	Mep	Down	2	Port	1	ITU ICC	TRNSTN	meg000	0	1	2	0	00-C0-F2-21-B8-C6

```
>
```

Messages: *Invalid parameter error returned from MEP*

Note: The S3280 supports a maximum of 10 MEPS per port assignable to any VLAN(s) on a port and a maximum of 80 MEPS per S3280. The maximum number of MEPs at each CCM interval that can be supported without affecting performance depends on what else is configured on the S3280.

Command: MEP Peer MEP

Syntax: **mep peer mep** [<inst>] [<mep>] [<mac_addr>] [enable|disable]

Description: Add, edit, or display a Peer MEP ID configuration, where:

<inst> : Instance number of this MEP.

<mep> : This MEP ID (0 - 0x1FFF).

<mac_addr> : MAC address (xx-xx-xx-xx-xx-xx).

enable/disable : enable/disable peer MEP.

Example 1:

```
>mep peer mep

MEP Peer MEP Configuration is:
  Inst      Peer id      Peer MAC
  -----
>MEP>peer mep 1 1 11-22-33-44-55-66 enable
>MEP>peer mep

MEP Peer MEP Configuration is:
  Inst      Peer id      Peer MAC
  -----
  1          1          11-22-33-44-55-66

MEP>
```

Example 2:

```
>mep peer mep

MEP Peer MEP Configuration is:
  Inst      Peer id      Peer MAC
  -----
  1          0          00-00-00-00-00-00
  2          1          00-00-00-00-00-00

>
```

Command: MEP Continuity Check Config

Syntax: **mep cc config** [<inst>] [<prio>] [300s|100s|10s|1s|6m|1m|6h] [enable|disable]

Description: Add, edit or display MEP Continuity Check configuration, where:

<inst> : The MEP Instance number.

<prio> : OAM PDU priority.

300s|100s|10s|1s|6m|1m|6h: OAM period (100s -> 100 PDU per second).

enable/disable : enable/disable MEP CC configuration.

Example:

```
MEP>cc config 1 1 10s enable
MEP>cc config

MEP CC Configuration is:
  Inst      Prio      Period
  -----
  1          1          10s

MEP>
```

Command: MEP Loss Measurement Config

Syntax: **mep lm config** [<inst>] [<prio>] [uni|multi] [single|dual] [300s|100s|10s|1s|6m|1m|6h] [<flr>] [enable|disable]

Description: Add, edit, or display MEP Loss Measurement configuration, where:

<inst> : MEP Instance number.
 <prio> : OAM PDU priority.
 uni|multi : Set Destination address to unicast or multicast.
 single|dual : LM is single-ended or dual-ended.
 300s|100s|10s|1s|6m|1m|6h: OAM period (100s -> 100 PDU per second).
 <flr> : Frame loss ratio (in seconds). The valid range is 0-65535 seconds.
 enable|disable : enable/disable MEP Loss Measurement.

Example: MEP>lm config 1 2 uni single 10s 4 enable

MEP>lm config

MEP LM Configuration is:

Inst	Prio	Cast	Ended	Period	Flr
1	2	Uni	Single	10s	4

MEP>

Command: MEP Automatic Protection Switching Config

Syntax: **mep aps config** [<inst>] [<prio>] [uni|multi] [laps|raps] [<octet>] [enable|disable]

Description: Add, edit or display MEP APS configuration. ETH-APS can be either linear APS or Ring APS. The parameters are:

<inst> : MEP Instance number.
 <prio> : OAM PDU priority.
 uni|multi : Destination address is unicast or multicast.
 laps|raps : Selection of Linear or Ring APS type (ELPS/LAPS or ERPS/RAPS protocol).
 <octet> : The last octet in RAPS multicast MAC..
 enable|disable: enable/disable MEP APS.

Example: MEP>aps config 1 2 uni laps 11 enable

MEP>aps config

MEP APS Configuration is:

Inst	Prio	Cast	Type	Octet
1	2	Uni	laps	B

MEP>aps config 1 0 uni raps 11 enable

MEP>aps config

MEP APS Configuration is:

Inst	Prio	Cast	Type	Octet
1	0	Uni	raps	B

MEP>

Messages: Invalid parameter error returned from MEP

MEP instance is not enabled

Command: MEP Client Config

Syntax: **mep client config** [<inst>] [domport|domevc] [<level>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>]

Description: Displays the current MEP Client configuration. The displayed parameters are:

<inst> : The Instance number.

domport|domevc: The Flow domain (the client domain - must be EVC).

<level> : The MEP level (0-7). This is the client MEG level - the contained level in the AIS and LCK frames.

<cflow> : The client flow instance number (EVC). This is the client flow instance - up to 10 possible client flows (EVC). The valid range is 0 - 65535.

Example: >mep client conf

```
MEP Client Configuration is:
  Inst      Domain      Level      Flows
    1        Port         0
    2        Port         0
    3        Port         0
    4        Port         0
>
```

Messages: 'instance' required

Command: MEP Alarm Indication Signal Config

Syntax: **mep ais config** [<inst>] [<prio>] [1s|1m] [protection] [enable|disable]

Description: Add, edit or display MEP AIS (Alarm Indication Signal) configuration, where:

<inst> : MEP Instance number.

<prio> : OAM PDU priority.

1s|1m : Transmit period for both AIS and LCK.

1s - to send OAM Frames in the rate of 1 frame-per-second (fps).

1m - to send OAM frames in the rate of 1 frame-per-minute (fps).

protection : Whether corresponding AIS leads to protection switching or not.

enable/disable: enable/disable MEP AIS configuration (insertion of AIS PDU transmission in client layer flows) can be enable/disabled here.

Example: MEP>ais config 1 2 1m clear enable
MEP>

Messages: Invalid parameter error returned from MEP
MEP instance is not enabled

Command: **MEP Link Trace Config**

Syntax: **mep lt config** [<inst>] [<prio>] [<mac_addr>] [<mep>] [<tll>] [enable|disable]

Description: Add, edit or display the MEP LT (Link Trace) configuration, where:

<inst> : MEP Instance number.

<prio> : OAM PDU priority. The priority (PCP) of the transmitted LTM frame.

[<mac_addr>]: The target machine's MAC address. The unicast MAC of the target MEP/MIP. MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxx xxxxxxxx', where x is a hexadecimal digit)

<mep> : MEP id (0-0x1FFF) - the peer MEP-ID of target MEP - only used if 'mac_addr' is 'all zeros'.

<tll> : LT - Time To Live; the TLL in the transmitted LTM (0-255).

enable|disable: enable/disable MEP Link Trace. Link Trace based on transmitting/receiving LTM/LTR PDU can be enabled/disabled. Link Trace is automatically disabled when all 5 transactions are done with 5 sec. interval - waiting 5 sec. for all LTR in the end. The LTM PDU is always transmitted as Multi-cast Class 2.

Example: `MEP>lt config 1 2 11-22-33-44-55-66 1 4`

'instance' and 'enable|disable' required

`MEP>lt config 2 2 11-22-33-44-55-66 1 4 enable`

Invalid number of peer's for this configuration

MEP>

`>mep lt config 1 1 11-22-33-44-55-66 1 1 enable`

`>mep lt config`

MEP LT Configuration is:

Inst	Prio	Mep	MAC	Ttl
1	1	1	11-22-33-44-55-66	1

>

Messages: *'instance' and 'enable/disable' required*

Invalid number of peer's for this configuration

MEP instance is not enabled

Command: MEP Loopback Config

Syntax: **mep lb config** [<inst>] [set|clear] [<prio>] [uni|multi] [<mac_addr>] [<mep>] [<tosend>] [<size>] [<gap>] [enable|disable]

Description: Add, edit, or display the MEP Loop Back (LB) configuration, where:

- <inst> : Instance number of this MEP.
- set|clear : OAM DEI set/clear ('set|clear' is set or clear of DEI of transmitted LBM frame).
- <prio> : OAM PDU priority ('prio' is the priority (PCP) of transmitted LBM frame).
- uni|multi : Destination address is unicast or multicast ('uni|multi' is for selecting uni-cast or multi-cast transmission of LBM frame).
- <mac_addr> : MAC address (xx-xx-xx-xx-xx-xx) (the unicast MAC of target MEP/MIP).
- <mep> : This MEP ID (0-0x1FFF) (the peer MEP-ID of target MEP - only used if 'mac_addr' is 'all zeros').
- <tosend> : Number of LBMs to send ('tosend' is the number of Loop Back Messages to be sent). The valid range is 1-1000 LBMs.
- <size> : Size of LBM data field in bytes. The valid range is 1-1400 bytes.
- <gap> : Gap between Loop Back Messages to send in 10ms increments. The valid range is 0-100, where '0' is as fast as possible. The 'gap' is the gap between LBMs.
- enable|disable: Enable or disable MEP Loop Back (LB) operation.

Example:

```
MEP>lb config 1 set 4 uni 11-22-33-44-55-66 1 16 100 1 enable
MEP>lb config
```

MEP LB Configuration is:

Inst	Dei	Prio	Cast	Mep	MAC	ToSend	Size	Gap
1			uni	4	11-22-33-44-55-66	1	16	100

```
MEP>
```

Messages: *'instance' and 'enable/disable' required*
Invalid number of peer's for this configuration
MEP instance is not enabled

Command: MEP Delay Measurement Config

Syntax: **mep dm config** [<inst>] [<prio>] [uni|multi] [<mep>] [oneway|twoway] [std|prop] [rdtrp|flow] [<gap>] [<count>] [us|ns] [keep|reset] [d2ford1] [enable|disable]

Description: Add, edit or display the MEP Delay Measurement configuration, where:

- <inst>** : Instance number for this MEP DM config.
- <prio>** : OAM PDU priority ('prio' is the priority (PCP) of transmitted DM frame).
- uni|multi** : Destination address is unicast or multicast ('uni|multi' is for selecting uni-cast or multi-cast transmission of DM frame).
- <mep>** : This MEP ID (0 - 0x1FFF). (The 'mep' is the peer MEP-ID of target MEP - only used if 'uni' is selected above).
- oneway|twoway** : DM is one-way or two-way. Enter 'oneway' for one-way (1DM) or enter 'twoway' for two-way (DMM) DM.
- std|prop** : Standard or proprietary way (w/ follow-up packets) to send DM ('std|prop' selects standardized or proprietary DM. The latest is using an off-standard follow-up message carrying the exact HW transmit timestamp).
- rdtrp|flow** : 2/4 timestamps selection ('rdtrp|flow' selects round-trip or flow delay calculation. Round-trip is not using the far-end timestamps to calculate the far-end residence time).
- <gap>** : Gap between 1DM/DMM to send in 10ms increments. The 'gap' is the interval between transmitting 1DM/DMM PDU - in 10 ms increments. The valid range is 10-65535.
- <count>** : The number of last records to calculate. The 'count' is the number of frames used for average calculation on the latest 'count' frames received. The valid range is 10-2000 frames.
- us|ns** : Time resolution; 'us|ns' calculation results are shown in micro or nano seconds.
- keep|reset** : The action to counter when overflow happens ('keep|reset' the action in case of total delay counter overflow - either 'keep' all results or 'reset' all results).
- d2ford1** : Enable to use DMM/DMR packets to calculate one-way DM. The 'd2ford1' is selected to used two-way DMM for calculate one-way delay. Select 'd2ford1' to used two-way DMM for calculate one-way delay.
- enable|disable**: Enable or disable MEP Delay Measurement operation. Default is disabled.

Example:

```
MEP>dm config 1 4 uni 1 oneway std rdtrp 10 100 us keep d2ford1 enable
MEP>dm config
```

MEP DM Configuration is:

Count	Inst	Unit	Prio	D2ford1	Cast	Mep	Way	Prtcl	2-way	Calc	Gap
					CNT	OV	ACT				
100	1	us	4	Enabled	Uni	1	One-way	Std		Rdtrp	10
						keep					

MEP>

Messages: *'instance' and 'enable/disable' required*
Invalid number of peer's for this configuration
MEP instance is not enabled

Command: MEP Test Config

Syntax: **mep tst config** [<inst>] [set|clear] [<prio>] [<mep>] [<rate>] [<size>] [allzero|allone|onezero] [enable|disable]

Description: Configure the MEP Test (Tst) Signal. The Ethernet Test Signal (ETH-Test) functions as a means for performing one-way in-service or out-of-service diagnostic testing between a pair of MEPs. The MEF 30 requirements define default protocol values and the protocol options required for a compliant MEF Service OAM implementation. Note that when performing out-of-service diagnostic testing, the ETH-LCK is used in conjunction with ETH-Test. The parameters are:

<inst> : Instance number for this MEP Test.
 set|clear : OAM DEI set/clear (set or clear DEI of transmitted LBM frames).
 <prio> : OAM PDU priority. The 'prio' is the priority (PCP) of transmitted TST frame.
 <mep> : This MEP ID (0-0x1FFF). (The 'mep' is the peer MEP-ID of a target MEP - only used if 'mac_addr' is 'all zeros').
 <rate> : Transmission bit rate of TST frames in Mbps. The 'rate' is the TST frame transmission bit rate in Mbps'. The valid range is 1-400 Mbps.
 <size> : Size of TST data field in bytes. (The 'size' is the size of the un-tagged TST frame - four bytes will be added for each tag.) This is entered as the wanted size (in bytes) of a un-tagged frame containing TST OAM PDU - including CRC (four bytes). For example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes . The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC. The transmitting frame rate will be adjusted according to the actually transmitted frame size to obtain correct transmission bit rate. The valid range is 1-1518.

allzero|allone|onezero: Data pattern to be filled in TST PDU. This is the pattern contained in the TST frame data TLV ('allzero' = 000 pattern; 'alone' = 111 pattern; 'onezero' = alternating 010 pattern). The 'empty' TST PDU has the size of 12 bytes. In order to achieve the configured frame size a data TLV will be added with a pattern. For example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes The TST PDU needs to be 46 bytes so a pattern of 46-12=34 bytes will be added.

enable|disable : Enable or disable MEP Test operation.

Example:

```
MEP>tst config 1 set 6 1 9 1000 onezero enable
MEP>tst config
```

MEP TST Configuration is:

Inst	Dei	Prio	Mep	rate	Size	Pattern	Sequence
1	1	6	1	9	1000	0xAA	

>

Messages:

Invalid parameter error returned from MEP

MEP instance is not enabled

Command: **MEP State**
Syntax: **mep state** [<inst>]
Description: Display the current MEP state, where:
 <inst>: Instance number for this MEP.

Example 1:

```
MEP>state
MEP state is:
      Inst      cLevel      cMeg      cMep      cAis      cLck      cSsf
  aBlk  aTsf  Peer MEP      cLoc      cRdi      cPeriod      cPrio
      1      False      False      False      False      False      True
False  True      1      False      False      False      False
      2      False      False      False      False      False      False
False  False
```

MEP>

Example 2:

```
>mep state
MEP state is:
  Inst  cLevel  cMeg  cMep  cAis  cLck  cSsf  aBlk  aTsf  Peer MEP  cLoc  cRdi  cPeriod  cPrio
  1  False  False  False  False  False  True  False  True
  2  False  False  False  False  False  True  False  True
```

>

The MEP state parameters are:

cLevel: Fault Cause indicating that a CCM is received with a lower level than the level configured for this MEP.

cMEG: Fault Cause indicating that a CCM is received with a MEG ID different from configured for this MEP.

cMEP: Fault Cause indicating that a CCM is received with a MEP ID different from all 'Peer MEP ID' configured for this MEP.

cAIS: Fault Cause indicating that AIS PDU is received. Ethernet alarm indication signal function (ETH-AIS) allows a customer who deploys an Ethernet service to tell if a connectivity fault exists at the current level or at a level below.

cLCK: Fault Cause indicating that LCK PDU is received. The Ethernet lock signal function is used to signal administrative locking of a server (sub) layer MEP and interruption of data traffic forwarding toward the MEP waiting for the traffic. The transmission and reception of LCK frames is similar to that of AIS frames except that with cLCK, the condition communicated is an administrative locking condition and not a defect condition.

cSSF: Fault Cause indicating that the server layer is indicating Signal Fail.

aBLK: The consequent action of blocking service frames in this flow is active.

aTSF: The consequent action of indicating Trail Signal Fail towards protection is active.

Peer MEP: This value will become an expected MEP ID in a received CCM.

cLoc: Fault Cause indicating that no CCM has been received (in 3,5 periods) from this peer MEP.

cRdi: Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP. Both 802.1ag and Y.1731 specify Ethernet Remote Defect Indication function (ETH-RDI).

cPeriod: Fault Cause indicating that a CCM is received with a period different than what is configured for this MEP - from this peer MEP.

cPrio: Fault Cause indicating that a CCM is received with a priority different than what is configured for this MEP from this peer MEP.

Command: MEP LOCK Config**Syntax:** **mep lck config** [<inst>] [<prio>] [1s|1m] [enable|disable]**Description:** Add, edit or display a MEP LCK configuration, where:

<inst> : Instance number for this MEP Lock configuration.

<prio> : OAM PDU priority ('prio' is the priority (PCP) of transmitted AIS frame).

1s|1m : Transmit period for both AIS and LCK; select either:**1s** - to send OAM Frames at the rate of 1 frame-per-second (fps), or**1m** - to send OAM frames at the rate of 1 frame-per-minute (fpm).**enable|disable:** enable/disable the MEP LCK capability.

Example:

```
MEP>lck config 1 2 1s enable
Invalid parameter error returned from MEP
MEP>lck config 1 2 1m enable
Invalid parameter error returned from MEP
MEP>>MEP lck config
MEP LCK Configuration is:
    Inst      Prio      Period
>
```

Command: MEP LM State**Syntax:** **mep lm state** [<inst>]

Description: Display the current MEP Loss Measurement (LM) state. Loss Measurement (LM) offers a way for operators to determine the amount of frame loss in an Ethernet network, over an EVC for example. Specifically, it is the ratio between undelivered OAM frames and the total number of OAM frames transmitted during a specific time interval. ITU-T Y.1731 defines two types of LM: 1) Single-Ended, where LM messages are transmitted to another MEP, which includes transmission and reception frame counts in its response message. Here, only the LM initiator is able to derive frame loss from the counters (since it does not include its local counters in the initial LM message); and 2) Dual-Ended. Continuity Check messages are used to carry frame transmission and reception counters. In contrast to the single-ended approach, this approach allows all MEPs inside a ME to derive frame loss, instead of only the initiating node.

The parameters are:

<inst>: Instance number to display. With no entry, all LM instances are displayed.

Example:

```
MEP>lm state
MEP LM state is:
Inst      Tx      Rx      Near Count      Far Count      Near Ratio      Far Ratio
1         98760      0           0           0           0           0
2           0           0           0           0           0           0
MEP>
```

Command: MEP LM Clear

Syntax: mep lm clear <inst>

Description: Clear the current MEP Loss Measurement (LM) state, where:
 <inst>: Instance number to clear. With no entry, all LM instances are cleared.

Example:

```
MEP>lm clear 2
MEP>lm clear
Missing <inst> parameter

Syntax:
MEP lm clear <inst>
MEP> lm clear 2
MEP>lm state
MEP LM state is:
Inst Tx Rx Near Count Far Count Near Ratio Far Ratio
1 101630 0 0 0 0 0
2 0 0 0 0 0 0
MEP>
```

Command: MEP LT State

Syntax: mep lt state [<inst>]

Description: Display the current MEP Link Trace (LT) state, where:
 <inst>: Instance number to display. With no entry, all LT instances are displayed.

Example:

```
>mep lt state
MEP LT state is:
Inst Transaction ID Ttl Mode Direction Relayed Last MAC Next MAC

>mep lt state
MEP LT state is:
Inst Transaction ID Ttl Mode Direction Relayed
Last MAC Next MAC
1 1 2 3 4 5
>
```

Command: MEP LB State

Syntax: mep lb state [<inst>]

Description: Display the current MEP Loop Back state, where:
 <inst>: Instance number to display. With no **inst** entry, all LB instances are displayed.

Example:

```
>mep lb state
MEP LB state is:
Inst Transaction ID MAC Received Out Of Order
>
```

Command: **MEP DM Clear**

Syntax: **mep dm clear** <inst>

Description: Clear the current MEP Delay Measurement state, where:
<inst>: Instance number to clear. With no entry, all DM instances are cleared.

Example:

```
>mep dm clear
Missing <inst> parameter

Syntax:
MEP dm clear <inst>
>mep dm clear 1
>
```

Command: **MEP DM State**

Syntax: **mep dm state** [<inst>]

Description: Display the current MEP Delay Measurement (DM) state, which can be used for measuring delay in a Carrier Ethernet network. The unit of measurement is the round trip delay of a frame, measured from its first transmitted bit, until the reception of its last bit. Since a DM frame must be sent back to its originating node, LB messages are used. Frame delay is the difference, in microseconds, between the time an ETH-DM frame is sent and received. (Frame delay variation - the difference between consecutive frame delay values - also called “frame jitter” - is a different parameter.) Two types of DM can be identified:

One-way measurement: An initiating MEP includes a transmission timestamp in the Ethernet frame. The destination node will capture the frame reception timestamp, and compare both timestamps. Consequently, the clocks of the sending and receiving nodes must be synchronized;

Two-way measurement: In contrast to the one-way measurement, this DM type does not require clock synchronization. The initiating node still includes a timestamp in the Ethernet frame. After the destination node performs a loopback on the frame, the initiating node will receive the frame again. On reception, this node will capture the reception timestamp.

The difference between the timestamps can be calculated. The parameters are:

<inst>: MEP Instance number to display.

Example:

```
MEP>dm state 1
MEP DM state is:
RxT : Rx Timeout
RxE : Rx Error
AT : Average Total
AN : Average last N
AVT : Average Variation Total
AVN : Average Variation last N
OV : Overflow. The number of statistics overflow.

Inst  Tx    RxT  Rx   RxE  AT   AN   AVT  AVN  Max  Min  OV
One-way(time unit: us)
Far-end-to-near-end
1     0     0    0    0    0    0    0    0    0    0    0
Near-end-to-far-end
1     16824 0    0    0    0    0    0    0    0    0    0
Two-way(time unit: us)
1     0     0    0    0    0    0    0    0    0    0    0
One-way(time unit: ns)
Two-way(time unit: ns)
MEP>
```

Command: **MEP TEST State**

Syntax: **mep tst state** [<inst>]

Description: Displays the MEP Test Signal state. The RX rate is shown in 100 Kbps. The parameters are:
 <inst>: The MEP Test instance number to display. No entry displays all instances configured.

Example:

```
MEP>tst state 1
MEP TST state is:
    Inst TX frame count    RX frame count    RX rate    Test time
    1     0                0                0          0

MEP>tst state
MEP TST state is:
    Inst TX frame count    RX frame count    RX rate    Test time
    1     0                0                0          0
    2     0                0                0          0

MEP>
```

Command: **MEP TEST Clear**

Syntax: **mep tst clear** <inst>

Description: Clears the MEP Test Signal state. The parameters are:
 <inst>: MEP Test Signal instance number to clear.

Example:

```
MEP>tst clear 1
MEP>tst clear
Missing <inst> parameter

Syntax:
MEP tst clear <inst>
MEP>tst clear 2
MEP>
```

Parameter Descriptions

Instance: The ID of the MEP. Click on the ID of a MEP to enter its configuration page.

Domain:

* Port: This is a MEP in the Port Domain. 'Flow Instance' is a Port.

* Evc: This is a MEP in the EVC Domain. 'Flow Instance' is an EVC

Mode:

* MEP: This is a Maintenance Entity End Point.

* MIP: This is a Maintenance entity Intermediate Point.

Direction:

* Ingress: This is a Ingress (down) MEP - monitoring ingress traffic on 'Residence Port'.

* Egress: This is a Egress (up) MEP - monitoring egress traffic on 'Residence Port'.

Residence Port: The port where MEP is monitoring - see 'Direction' description above.

* Level: The MEG level of this MEP (0-7).

* Flow Instance: The MEP is related to this flow - See 'Domain' description above.

Tagged VID:

* Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID.

* EVC MEP: An inner C-tag is added with this VID.

* Entering '0' means no TAG added.

QoS Commands

QoS (Quality of Service) is a method to guarantee a bandwidth relationship between individual applications or protocols. A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required QoS becomes the secret to a successful end-to-end business solution, with QoS providing the set of techniques to manage network resources. The QCL (QoS Control List) is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects. Each accessible traffic object contains an identifier to its QCL. Each privilege sets a specific traffic object to a specific QoS class. The S3280 commands include:

>qos ?

Available Commands:

```

QoS Configuration [<port_list>]
QoS Port Classification Class [<port_list>] [<class>]
QoS Port Classification DPL [<port_list>] [<dpl>]
QoS Port Classification PCP [<port_list>] [<pcp>]
QoS Port Classification DEI [<port_list>] [<dei>]
QoS Port Classification Tag [<port_list>] [enable|disable]
QoS Port Classification Map [<port_list>] [<pcp_list>] [<dei_list>] [<class>] [<dpl>]
QoS Port Classification DSCP [<port_list>] [enable|disable]
QoS Port Policer Mode [<port_list>] [enable|disable]
QoS Port Policer Rate [<port_list>] [<rate>]
QoS Port Policer Unit [<port_list>] [kbps/fps]
QoS Port Policer FlowControl [<port_list>] [enable|disable]
QoS Port Policer Order [<port_list>] [<order>]
QoS Port QueuePolicer Mode [<port_list>] [<queue_list>] [enable|disable]
QoS Port QueuePolicer Rate [<port_list>] [<queue_list>] [<bit_rate>]
QoS Port Scheduler Mode [<port_list>] [strict|weighted]
QoS Port Scheduler Weight [<port_list>] [<queue_list>] [<weight>]
QoS Port Shaper Mode [<port_list>] [enable|disable]
QoS Port Shaper Rate [<port_list>] [<bit_rate>]
QoS Port QueueShaper Mode [<port_list>] [<queue_list>] [enable|disable]
QoS Port QueueShaper Rate [<port_list>] [<queue_list>] [<bit_rate>]
QoS Port QueueShaper Excess [<port_list>] [<queue_list>] [enable|disable]
QoS Port TagRemarking Mode [<port_list>] [classified|default|mapped]
QoS Port TagRemarking PCP [<port_list>] [<pcp>]
QoS Port TagRemarking DEI [<port_list>] [<dei>]
QoS Port TagRemarking Map [<port_list>] [<class_list>] [<dpl_list>] [<pcp>] [<dei>]
QoS Port DSCP Translation [<port_list>] [enable|disable]
QoS Port DSCP Classification [<port_list>] [none|zero|selected|all]
QoS Port DSCP EgressRemark [<port_list>] [disable|enable|remap_dp_unaware|remap_dp_aware]
QoS DSCP Map [<dscp_list>] [<class>] [<dpl>]
QoS DSCP Translation [<dscp_list>] [<trans_dscp>]
QoS DSCP Trust [<dscp_list>] [enable|disable]
QoS DSCP Classification Mode [<dscp_list>] [enable|disable]
QoS DSCP Classification Map [<class_list>] [<dpl_list>] [<dscp>]
QoS DSCP EgressRemap [<dscp_list>] [<dpl_list>] [<dscp>]
QoS Storm Unicast [enable|disable] [<packet_rate>]
QoS Storm Multicast [enable|disable] [<packet_rate>]
QoS Storm Broadcast [enable|disable] [<packet_rate>]
QoS QCL Add [<qce_id>] [<qce_id_next>] [<port_list>] [<tag>] [<vid>] [<pcp>] [<dei>] [<smac>] [<dmac_type>]
  [(etype [<etype>]) | (LLC [<DSAP>] [<SSAP>] [<control>]) | (SNAP [<PID>]) | (ipv4 [<protocol>] [<sip>] [<dscp>]
  [<fragment>] [<sport>] [<dport>]) |
  (ipv6 [<protocol>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])]]  [<class>] [<dp>] [<classified_dscp>]
QoS QCL Delete <qce_id>
QoS QCL Lookup [<qce_id>]
QoS QCL Status [combined|static|conflicts]
QoS QCL Refresh
>

```

Command: QoS Configuration**Syntax:** **qos configuration** [<port_list>]**Description:** Show the current QoS (Quality of Service) configuration, where:
<port_list>: Port list or 'All'. The default is 'All' ports. Note that this can be a long config list.**Example:** >**qos config 1**

```

QoS Configuration:
=====

QoS Port Classification:
=====

Port   PCP   DEI   QoS class   DP level   Tag class.
----   -
1      0     0     0           0          Disabled
:
:
:
QoS Storm Control:
=====

Storm Unicast   : Disabled      1 fps
Storm Multicast: Disabled      1 fps
Storm Broadcast: Disabled      1 fps

QoS QCL:
=====

Number of QCEs: 0

```

Command: QoS Port Classification Class**Syntax:** **qos port classification class** [<port_list>] [<class>]**Description:** Set or show the default QoS class. Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority. The parameters are:

<port_list>: Port list or 'all', default: All ports.

<class> : QoS class (0-7)

Example: >**qos port classification class 1 2**

```

>qos port classification class 2 2
>qos port classification class 3 3
>qos port classification class 4 4
>qos port classification class

Port   QoS class
----   -
1      2
2      2
3      3
4      4
5      0
6      0
7      0
8      0
>

```

Command: QoS Port Classification DPL (Drop Precedence Level)

Syntax: `qos port classification dpl [<port_list>] [<dpl>]`

Description: Set or show the default Drop Precedence Level, where:
 <port_list>: Port list or 'all', default: All ports.
 <dpl> : Drop Precedence Level (0-1).

Example:

```
>qos port classification dpl 1 0
>qos port classification dpl 2 0
>qos port classification dpl 3 1
>qos port classification dpl 4 1
>qos port classification dpl
```

Port	DP level
1	0
2	0
3	1
4	1
5	0
6	0
7	0
8	0

Command: QoS Port Classification PCP (Priority Code Point)

Syntax: `qos port classification pcp [<port_list>] [<pcp>]`

Description: Set or show the default PCP for an untagged frame, where:
 <port_list>: Port list or 'all', default: All ports.
 <pcp> : Priority Code Point (0-7)

Example:

```
>qos port classification pcp 1 4
>qos port classification pcp 2 5
>qos port classification pcp 3 6
>qos port classification pcp
```

Port	PCP
1	4
2	5
3	6
4	0
5	0
6	0
7	0
8	0

Command: QoS Port Classification DEI**Syntax:** `qos port classification dei [<port_list>] [<dei>]`**Description:** Set or show the default DEI (Drop Eligible Indicator) for an untagged frame, where:
<port_list>: Port list or 'all'. The default is 'All' ports.
<dei> : Drop Eligible Indicator (0-1).

Example:

```
>qos port classification dei

Port  DEI
----  ---
1     0
2     0
3     0
4     0
5     0
6     0
7     0
8     0
>qos port classification dei 1-3 1
>qos port classification dei

Port  DEI
----  ---
1     1
2     1
3     1
4     0
5     0
6     0
7     0
8     0
>
```

Command: QoS Port Classification Tag**Syntax:** `qos port classification tag [<port_list>] [enable|disable]`**Description:** Set or show if the classification is based on the PCP and DEI values in tagged frames, where:
<port_list>: Port list or 'all'. The default is 'All' ports.
enable : Enable tag classification
disable : Disable tag classification
(default: Show tag classification mode)

Example:

```
>qos port classification tag 1 enable
>qos port classification tag 2 enable
>qos port classification tag 3 enable
>qos port classification tag

Port  Tag class.
----  -
1     Enabled
2     Enabled
3     Enabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
>
```

Command: QoS Port Classification Map**Syntax:** **qos port classification map** [<port_list>] [<pcp_list>] [<dei_list>] [<class>] [<dpl>]**Description:** Set or show the port classification map. This map is used when port classification tag is enabled, and the purpose is to translate the Priority Code Point (PCP) and Drop Eligible Indicator (DEI) from a tagged frame to QoS class and DP level. The parameters are:

<port_list>: Port list or 'All'. The default is 'All ports'.

<pcp_list> : PCP list or 'All'. The default is 'All PCPs' (0-7).

<dei_list> : DEI list or 'All'. the default is 'All DEIs' (0-1).

<class> : QoS class (0-7).

<dpl> : Drop Precedence Level (0-1). The DPL for frames not classified in another way.

Example:

```
>qos port classification map 1 1 1 1 0
>qos port classification map 2 2 0 0 1
>qos port classification map 3 3 1 1 0
>qos port classification map 1,2
```

Port	PCP	DEI	QoS class	DP level
1	0	0	1	0
	0	1	1	1
	1	0	0	0
	1	1	1	0
	2	0	2	0
	2	1	2	1
	3	0	3	0
	3	1	3	1
	4	0	4	0
	4	1	4	1
	5	0	5	0
	5	1	5	1
	6	0	6	0
	6	1	6	1
	7	0	7	0
	7	1	7	1
2	0	0	1	0
	0	1	1	1
	1	0	0	0
	1	1	0	1
	2	0	0	1
	2	1	2	1
	3	0	3	0
	3	1	3	1
	4	0	4	0
	4	1	4	1
	5	0	5	0
	5	1	5	1
	6	0	6	0
	6	1	6	1
	7	0	7	0
	7	1	7	1

>

Command: QoS Port Classification DSCP**Syntax:** `qos port classification dscp [<port_list>] [enable|disable]`**Description:** Set or show if the classification is based on DSCP value in IP frames, where:

<port_list>: Port list or 'all', default: All ports.

enable : Enable DSCP based classification.**disable** : Disable DSCP based classification (the default setting).

(The default is 'Show DSCP based classification mode'.)

Example:

```
>qos Port Classification DSCP 1 enable
>qos Port Classification DSCP 2 enable
>qos Port Classification DSCP 3 enable
>qos Port Classification DSCP
Port   DSCP based class.
-----
1      Enabled
2      Enabled
3      Enabled
4      Disabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
>
```

Command: QoS Port Policer Mode**Syntax:** `qos port policer mode [<port_list>] [enable|disable]`**Description:** Set or show the port policer mode, where:

<port_list>: Port list or 'All'. The default is 'All ports'.

enable : Enable QoS port policer mode.**disable** : Disable QoS port policer mode (the default setting).

(The default is 'Show port policer mode'.)

Example:

```
>QoS Port Policer Mode
Port   Parm      Policer
-----
1      Mode      Disabled
2      Mode      Disabled
3      Mode      Disabled
4      Mode      Disabled
5      Mode      Disabled
6      Mode      Disabled
7      Mode      Disabled
8      Mode      Disabled
>QoS Port Policer Mode 1,2,3 enable
>QoS Port Policer Mode
Port   Parm      Policer
-----
1      Mode      Enabled
2      Mode      Enabled
3      Mode      Enabled
4      Mode      Disabled
5      Mode      Disabled
6      Mode      Disabled
7      Mode      Disabled
8      Mode      Disabled
>
```

Command: QoS Port Policer Rate

Syntax: **qos port policer rate** [<port_list>] [<rate>]

Description: Set or show the port policer rate, where:

<port_list>: Port list or 'All'. The default is 'All ports'.

<rate> : Rate in kbps or fps (100 - 3300000). The default is 500 kbps.

Example:

```
>QoS Port Policer Rate
Port  Parm      Policer
----  -
1     Rate      500 kbps
2     Rate      500 kbps
3     Rate      500 kbps
4     Rate      500 kbps
5     Rate      500 kbps
6     Rate      500 kbps
7     Rate      500 kbps
8     Rate      500 kbps
>QoS Port Policer Rate 1 1000
>QoS Port Policer Rate
Port  Parm      Policer
----  -
1     Rate      1000 kbps
2     Rate      500 kbps
3     Rate      500 kbps
4     Rate      500 kbps
5     Rate      500 kbps
6     Rate      500 kbps
7     Rate      500 kbps
8     Rate      500 kbps
>
```

Command:

QoS Port Policer Unit

Syntax: **qos port policer unit** [<port_list>] [kbps|fps]

Description: Set or show the port policer unit, where:

<port_list>: Port list or 'All'. The default is 'All ports'.

kbps : Unit is kilo bits per second (the default).

fps : Unit is frames per second.

(The default is 'Show port policer unit'.)

Example:

```
>QoS Port Policer Unit 1 kbps
>QoS Port Policer Unit
Port  Parm      Policer
----  -
1     Unit      kbps
2     Unit      kbps
3     Unit      kbps
4     Unit      kbps
5     Unit      kbps
6     Unit      kbps
7     Unit      kbps
8     Unit      kbps
>
```

Command: QoS Port Policer FlowControl

Syntax: qos port policer flowcontrol [<port_list>] [enable|disable]

Description: Set or show the port policer flow control. If policer flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames. The parameters:
 <port_list>: Port list or 'All'. The default is 'All' ports.

enable : Enable port policer flow control.

disable : Disable port policer flow control (the default).

(The default is 'Show port policer flow control mode'.)

Example: >QoS Port Policer FlowControl 1 enable

>QoS Port Policer FlowControl

Port	Parm	Policer
1	Flow Ctl	Enabled
2	Flow Ctl	Disabled
3	Flow Ctl	Disabled
4	Flow Ctl	Disabled
5	Flow Ctl	Disabled
6	Flow Ctl	Disabled
7	Flow Ctl	Disabled
8	Flow Ctl	Disabled

>

Command: Set / Show QoS Port Policer Order

Syntax: qos port policer order [<port_list>] [<order>]

Description: Set or show the Policer order mode, where:

<port_list> : Port list or 'all', default: All ports

<order>] : Policer Order configurations. The following orders are allowed based on mode selections:

1 : QoS Policer Order is Queue, then Port, and then ACL (default).

2 : QoS Policer Order is ACL, then Queue, and then Port.

The default is 'Show QoS Policer order'.

Example:

```
>qos port policer order

Port  Polier Order
----  -
1     1 (Queue Port ACL)
2     1 (Queue Port ACL)
3     1 (Queue Port ACL)
4     1 (Queue Port ACL)
5     1 (Queue Port ACL)
6     1 (Queue Port ACL)
7     1 (Queue Port ACL)
8     1 (Queue Port ACL)
>qos port policer order all 2
>qos port policer order

Port  Polier Order
----  -
1     2 (ACL Queue Port)
2     2 (ACL Queue Port)
3     2 (ACL Queue Port)
4     2 (ACL Queue Port)
5     2 (ACL Queue Port)
6     2 (ACL Queue Port)
7     2 (ACL Queue Port)
8     2 (ACL Queue Port)
>
```

Command: QoS Port QueuePolicer Mode**Syntax:** **qos port queuепolicer mode** [<port_list>] [<queue_list>] [enable|disable]**Description:** Set or show the port queue policer mode, where:

<port_list> : Port list or 'All'. The default is 'All' ports.

<queue_list>: Queue list or 'All'. The default is 'All queues' (0-7).

enable : Enable port queue policer.**disable** : Disable port queue policer.

(The default is 'Show port queue policer mode'.)

Example:

```
>qos port queuепolicer mode 1 enable
>qos port queuепolicer mode 1,2
```

Port	Queue	Mode
----	-----	-----
1	0	Enabled
	1	Enabled
	2	Enabled
	3	Enabled
	4	Enabled
	5	Enabled
	6	Enabled
	7	Enabled
2	0	Disabled
	1	Disabled
	2	Disabled
	3	Disabled
	4	Disabled
	5	Disabled
	6	Disabled
	7	Disabled

```
>
```

Command: QoS Port QueuePolicer Rate**Syntax:** **qos port queupolicer rate** [<port_list>] [<queue_list>] [<bit_rate>]**Description:** Set or show the port queue policer rate, where:

<port_list> : Port list or 'All'. The default is All ports.

<queue_list>: Queue list or 'All'. The default is 'All queues' (0-7).

<bit_rate> : Rate in kilo bits per second (100-3300000 kbps).

Example:

```
>qos port queupolicer rate 1,2,3 1 5000
>qos port queupolicer rate 1,2,3
```

Port	Queue	Rate
1	0	500 kbps
	1	5000 kbps
	2	500 kbps
	3	500 kbps
	4	500 kbps
	5	500 kbps
	6	500 kbps
	7	500 kbps
2	0	500 kbps
	1	5000 kbps
	2	500 kbps
	3	500 kbps
	4	500 kbps
	5	500 kbps
	6	500 kbps
	7	500 kbps
3	0	500 kbps
	1	5000 kbps
	2	500 kbps
	3	500 kbps
	4	500 kbps
	5	500 kbps
	6	500 kbps
	7	500 kbps

```
>
```

Command: **QoS Port Scheduler Mode**
Syntax: **qos port scheduler mode** [<port_list>] [strict|weighted]
Description: Set or show the port scheduler mode, where:
<port_list>: Port list or 'all'. The default is 'All' ports.
strict : Strict port scheduler mode (the default).
weighted: Weighted port scheduler mode.
(The default is 'Show port scheduler mode'.)

Example:

```
>qos port scheduler mode 1,2,3 weighted
>qos port scheduler mode

Port  Mode
----  -
1     Weighted
2     Weighted
3     Weighted
4     Strict
5     Strict
6     Strict
7     Strict
8     Strict
>
```

Command: QoS Port Scheduler Weight**Syntax:** `qos port scheduler weight [<port_list>] [<queue_list>] [<weight>]`**Description:** Set or show the port scheduler weight, where:

<port_list> : Port list or 'all'. The default is 'All' ports.

<queue_list>: Weighted queue list or 'All'. The default is 'All' weighted queues (0-5).

<weight> : Scheduler weight (1-100).

Example:

```
>qos port scheduler weight 1,2,3 all 50
>qos port scheduler weight 1,2,3 all 50
>qos port scheduler weight 1,2,3,4
```

Port	Queue	Weight
1	0	50 (17%)
	1	50 (17%)
	2	50 (17%)
	3	50 (17%)
	4	50 (17%)
	5	50 (17%)
2	0	50 (17%)
	1	50 (17%)
	2	50 (17%)
	3	50 (17%)
	4	50 (17%)
	5	50 (17%)
3	0	50 (17%)
	1	50 (17%)
	2	50 (17%)
	3	50 (17%)
	4	50 (17%)
	5	50 (17%)
4	0	75 (17%)
	1	75 (17%)
	2	75 (17%)
	3	75 (17%)
	4	75 (17%)
	5	75 (17%)

>

Command: QoS Port QueueShaper Mode**Syntax:** **qos port queueshaper mode** [<port_list>] [<queue_list>] [enable|disable]**Description:** Set or show the port queue shaper mode, where:

<port_list> : Port list or 'all', default: All ports.

<queue_list>: Queue list or 'All'. The default is 'All' queues (0-7).

enable : Enable port queue shaper.**disable** : Disable port queue shaper (default).

(The default is 'Show port queue shaper mode'.)

Example:

```
>qos port queueshaper mode 1 1 enable
>qos port queueshaper mode 2 1 disable
>qos port queueshaper mode 1,2
```

Port	Queue	Mode
1	0	Disabled
	1	Enabled
	2	Disabled
	3	Disabled
	4	Disabled
	5	Disabled
	6	Disabled
	7	Disabled
2	0	Disabled
	1	Disabled
	2	Disabled
	3	Disabled
	4	Disabled
	5	Disabled
	6	Disabled
	7	Disabled

```
>
```

Command: QoS Port QueueShaper Rate**Syntax:** **qos port queueshaper rate** [<port_list>] [<queue_list>] [<bit_rate>]**Description:** Set or show the port queue shaper rate, where:

<port_list> : Port list or 'All'. The default is 'All ports'.

<queue_list>: Queue list or 'All'. The default is 'All queues' (0-7).

<bit_rate> : Rate in kilo bits per second (100 - 3300000 kbps).

Example:

```
>qos port queueshaper rate 1 1 3300000
>qos port queueshaper rate 1 2 50000
>qos port queueshaper rate 1 3 100000
>qos port queueshaper rate 1 4 6660000
Invalid parameter: 6660000
```

Syntax:

QoS Port QueueShaper Rate [<port_list>] [<queue_list>] [<bit_rate>]

>qos port queueshaper rate 1 4 666000

>qos port queueshaper rate 1

Port	Queue	Rate
1	0	500 kbps
	1	3300 Mbps
	2	50 Mbps
	3	100 Mbps
	4	666 Mbps
	5	500 kbps
	6	500 kbps
	7	500 kbps

Command: QoS Port QueueShaper Excess**Syntax:** **qos port queueshaper excess** [<port_list>] [<queue_list>] [enable|disable]**Description:** Set or show the port queue excess bandwidth mode, where:

<port_list> : Port list or 'All'. The default is 'All ports'.

<queue_list>: Queue list or 'All'. The default is 'All queues' (0-7).

enable : Enable use of excess bandwidth.**disable** : Disable use of excess bandwidth (the default).

(The default is 'Show port queue excess bandwidth mode'.)

Example:

```
>qos port queueshaper excess 1 1 enable
>qos port queueshaper excess 1 2 enable
>qos port queueshaper excess 1 3 enable
>qos port queueshaper excess 1
```

Port	Queue	Excess
1	0	Disabled
	1	Enabled
	2	Enabled
	3	Enabled
	4	Disabled
	5	Disabled
	6	Disabled
	7	Disabled

Command: QoS Port Shaper Mode

Syntax: **qos port shaper mode** [<port_list>] [enable|disable]

Description: Set or show the port shaper mode, where:
 <port_list>: Port list or 'All'. The default is 'All ports'.
enable : Enable port shaper.
disable : Disable port shaper (the default).
 (The default is 'Show port shaper mode'.)

Example:
 >**qos port shaper mode 1,2,3 enable**
 >**qos port shaper mode**

```
Port  Mode
----  -
1     Enabled
2     Enabled
3     Enabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
>
```

Command: **QoS Port Shaper Rate**

Syntax: **qos port shaper rate** [<port_list>] [<bit_rate>]

Description: Set or show the port shaper rate, where:
 <port_list>: Port list or 'All'. The default is 'All ports'.
 <bit_rate> : Rate in kilo bits per second (100 - 3300000 kbps).The default is 500 kbps.

Example:
 >**qos port shaper rate 1 500**
 >**qos port shaper rate 2 1500**
 >**qos port shaper rate 3 75000**
 >**qos port shaper rate**

```
Port  Rate
----  -
1     500 kbps
2     75 Mbps
3     75 kbps
4     500 kbps
5     500 kbps
6     500 kbps
7     500 kbps
8     500 kbps
>
```


Command: QoS Port TagRemarking Mode**Syntax:** `qos port tagremarking mode [<port_list>] [classified|default|mapped]`

Description: Set or show the port tag remarking mode, where:
 <port_list>: Port list or 'All'. The default is 'All ports'.
classified: Use classified PCP/DEI values.
default : Use default PCP/DEI values.
mapped : Use mapped versions of QoS class and DP level.
 (The default is: 'Show port tag remarking mode'.)

Example:

```
>qos port tagremarking mode 2 classified
>qos port tagremarking mode 3 mapped
>qos port tagremarking mode 4 mapped
>qos port tagremarking mode 5 mapped
>qos port tagremarking mode

Port  Mode
----  -
1     Default
2     Classified
3     Mapped
4     Mapped
5     Mapped
6     Default
7     Default
8     Default
>
```

Command: QoS Port TagRemarking PCP (Priority Code Point)**Syntax:** `qos port tagremarking pcp [<port_list>] [<pcp>]`

Description: Set or show the default PCP. This value is used when 'port tag remarking mode' (above) is set to 'default'. The parameters are:
 <port_list>: Port list or 'All'. The default is 'All ports'.
 <pcp> : Priority Code Point (0-7). The default is '0'.

Example:

```
>qos port tagremarking pcp 3,4,5 4
>qos port tagremarking pcp

Port  PCP
----  ---
1     0
2     0
3     4
4     4
5     4
6     0
7     0
8     0
>
```

Command: QoS Port TagRemarking DEI**Syntax:** **qos port tagremarking dei** [<port_list>] [<dei>]**Description:** Set or show the default DEI (Drop Eligible Indicator). This value is used when the 'port tag remarking mode' is set to 'default'. The parameters are:

<port_list>: Port list or 'All'. The default is 'All' ports.

<dei> : Drop Eligible Indicator (0-1). The default is '0'.

Example:

```
>qos port tagremarking dei 3 1
>qos port tagremarking dei 2 1
>qos port tagremarking dei 1 1
>qos port tagremarking dei
```

Port	DEI
----	----
1	1
2	1
3	1
4	0
5	0
6	0
7	0
8	0

Command: QoS Port TagRemarking Map**Syntax:** **qos port tagremarking map** [<port_list>] [<class_list>] [<dpl_list>] [<pcp>] [<dei>]**Description:** Set or show the port tag remarking map. This map is used when port tag remarking mode is set to 'mapped', and the purpose is to translate the classified QoS class (0-7) and DP level (0-1) to PCP and DEI. The parameters are:

<port_list> : Port list or 'All'. The default is 'All' ports.

<class_list>: QoS class list or 'All'. The default is 'All' QoS classes (0-7).

<dpl_list> : DP level list or 'all', default: All DP levels (0-1).

<pcp> : Priority Code Point (0-7).

<dei> : Drop Eligible Indicator (0-1).

Example:

```
>qos port tagremarking map 1
```

Port	QoS class	DP level	PCP	DEI
----	-----	-----	----	----
1	0	0	1	0
	0	1	1	1
	1	0	0	0
	1	1	0	1
	2	0	2	0
	2	1	2	1
	3	0	3	0
	3	1	3	1
	4	0	4	0
	4	1	4	1
	5	0	5	0
	5	1	5	1
	6	0	6	0
	6	1	6	1
	7	0	7	0
	7	1	7	1

Command: QoS Port DSCP Translation**Syntax:** **qos port dscp translation** [<port_list>] [enable|disable]**Description:** Set or show DSCP ingress translation mode. If translation is enabled for a port, the incoming frame DSCP value is translated and that translated value is used for QoS classification.

The parameters are:

<port_list>: Port list or 'All'. The default is 'All' ports.

enable : Enable DSCP ingress translation.**disable** : Disable DSCP ingress translation. The default is 'disabled'.

(The default is 'Show DSCP ingress translation mode'.)

Example:
>qos port dscp translation 1,2,3 enable
>qos port dscp translation

```

Port   DSCP trans.
-----
1      Enabled
2      Enabled
3      Enabled
4      Disabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
>

```

Command: QoS Port DSCP Classification**Syntax:** **qos port dscp classification** [<port_list>] [none|zero|selected|all]**Description:** Set or show DSCP classification based on QoS class and DP level. This enables per port to map new DSCP value based on QoS class and DP level. The parameters are:

<port_list>: Port list or 'All'. The default is 'All' ports.

none : No DSCP ingress classification.**zero** : Classify DSCP if DSCP = 0.**selected** : Classify DSCP for which class. mode is 'enable'.**all** : Classify all DSCP.

(The default is 'Show port DSCP ingress classification mode'.)

Example:
>qos port dscp classification 1 zero
>qos port dscp classification 2,3 selected
>qos port dscp classification 4-8 all
>qos port dscp classification

```

Port   Ingress class.
-----
1      DSCP = 0
2      Selected
3      Selected
4      All
5      All
6      All
7      All
8      All
>

```

Command: QoS Port DSCP EgressRemark**Syntax:** **qos port dscp egressremark** [<port_list>][disable|enable|remap_dp_unaware|remap_dp_aware]**Description:** Set or show the port DSCP remarking mode, where:

<port_list>: Port list or 'All'. The default is 'All' ports.

disable : Disable DSCP egress rewrite. The default is disabled.**enable** : Enable DSCP egress rewrite with the value received from analyzer**remap_dp_unaware** : Rewrite DSCP in egress frame with remapped DSCP where remap is DP unaware or DP = 0.**remap_dp_aware** : Rewrite DSCP in egress frame with remapped DSCP where remap is DP aware and DP = 1.

(The default is 'Show port DSCP egress remarking mode'.)

Example:

```
>qos Port DSCP EgressRemark 1-3 enable
>qos Port DSCP EgressRemark

Port  Rewrite
-----
1     Enabled
2     Enabled
3     Enabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
>
```

Command: QoS DSCP Map**Syntax:** **qos dscp map** [<dscp_list>] [<class>] [<dpl>]**Description:** Set or show DSCP mapping table. This table is used to map QoS class and DP level based on DSCP value. DSCP value used to map QoS class and DPL is either translated DSCP value or incoming frame DSCP value. The parameters are:

<dscp_list>: DSCP (0-63) list or 'All'.

(The default is 'Show DSCP ingress map table' (i.e., DSCP->(class, DPL)).

<class> : QoS class (0-7).

<dpl> : Drop Precedence Level (0-1).

Example:

```
>qos dscp map 1 5 1
>qos dscp map 2 3 1
>qos dscp map 3 4 0
>qos dscp map 1-3

DSCP      QoS Class  DP Level
-----
1         5          1
2         3          1
3         4          0
>
```

Command: QoS DSCP Translation**Syntax:** **qos dscp translation** [<dscp_list>] [<trans_dscp>]

Description: Set or show global ingress DSCP translation table. If port DSCP translation is 'enabled', the translation table is used to translate incoming frames DSCP value and the translated value is used to map QoS class and DP level. The maximum number of supported DSCP values is 64. The DSCP Name can be BE, CSx, EFx, or AFx where:

AF (Assured Forwarding) is provided in four classes for bursty real and non-real time services.

BE: refers to Standard (Best Effort) forwarding.

CS refers to the Class Selector (per RFC 2474).

EF refers to the Expedited Forwarding (RFC 3246). The EF PHB has the characteristics of low delay, low loss and low jitter. These characteristics are suitable for voice, video and other real-time services.

The parameters are:

<**dscp_list**> : DSCP (0-63) list or 'All'.
(The default is 'Show DSCP translation table'.)

<**trans_dscp**>: Translated DSCP: 0-63, BE, CS1-CS7, EF or AF11-AF43.

Example:

```
>QoS dscp translation 1-4
DSCP      Ingr. Trans.
-----
1          1
2          2
3          3
4          4
>QoS dscp translation 1 be
>QoS dscp translation 2 CS1
>QoS dscp translation 1-4
DSCP      Ingr. Trans.
-----
1          0   (BE)
2          8   (CS1)
3          3
4          4
>
```

Command: QoS DSCP Trust**Syntax:** **qos dscp trust** [<dscp_list>] [enable|disable]**Description:** Set or show whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and DPL. Frames with untrusted DSCP values are treated as a non-IP frame. The parameters are:

<dscp_list>: DSCP (0-63) list or 'All'.

enable : Set DSCP as trusted DSCP.**disable** : Set DSCP as un-trusted DSCP.

(The default is 'Show DSCP Trust status'.)

Example:

```
>qos dscp trust 0 enable
>qos dscp trust 0,1
DSCP      Trust
-----
0 (BE)    Enabled
1         Disabled
>
```

Command: QoS DSCP Classification Mode**Syntax:** **qos dscp classification mode** [<dscp_list>] [enable|disable]**Description:** Set or show DSCP ingress classification mode. If port DSCP classification is 'selected', DSCP will be classified based on QoS class and DP level only for DSCP value with classification mode 'enabled'. DSCP may be translated DSCP if translation is enabled for the port.

The parameters are:

<dscp_list>: DSCP (0-63) list or 'All'.

enable : Enable DSCP ingress classification.**disable** : Disable DSCP ingress classification.

(The default is 'Show DSCP classification mode'.)

Example:

```
>qos dscp classification mode 1-3 enable
>qos dscp classification mode 1-6
DSCP      Ingr. Classify
-----
1         Enabled
2         Enabled
3         Enabled
4         Disabled
5         Disabled
6         Disabled
>
```

Command: QoS DSCP Classification Map**Syntax:** **qos dscp classification map** [<class_list>] [<dpl_list>] [<dscp>]**Description:** Set or show DSCP ingress classification table. This table is used to map DSCP from QoS class and DP level. The DSCP which needs to be classified depends on port DSCP classification and DSCP classification mode. Incoming frame DSCP may be translated before using the value for classification. The parameters are:

<class_list>: QoS class list or 'All'. The default is 'All QoS classes' (0-7).

<dpl_list> : DP level list or 'All'. The default is 'All DP levels' (0-1).

<dscp> : Mapped DSCP: 0-63, BE, CS1-CS7, EF or AF11-AF43.

Example:

```
>qos dscp classification map 1 0 BE
>qos dscp classification map 1
QoS Class  DP Level  DSCP
-----
1           0          0  (BE)
1           1          0  (BE)
>
```

Note: The **dscp** parameter is the Diffserv Code Point value. It can be a specific value, range of values, or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43. Select Any, Specific, or Range. If Specific, specify the DSCP name (e.g., BE). If Range, specify the DSCP range (e.g., BE - 63).

Command: QoS DSCP EgressRemap**Syntax:** **qos dscp egressremap** [<dscp_list>] [<dpl_list>] [<dscp>]**Description:** Set or show DSCP egress remap table. This table is used if the port egress remarking mode is 'remap' and the purpose is to map the DSCP and DP level to a new DSCP value.

The parameters are:

<dscp_list>: DSCP (0-63) list or 'All'.

<dpl_list> : DP level list or 'All'. The default is 'All' DP levels (0-1).

<dscp> : Egress remapped DSCP: 0-63, BE, CS1-CS7, EF or AF11-AF43.

Example:

```
>qos dscp egressremap 1 0 BE
>qos dscp egressremap 2 0 EF
>qos dscp egressremap 1-4
DSCP      Egr. Remap-DP0  Egr. Remap-DP1
-----
1         0  (BE)       1
2         46  (EF)       2
3         3           3
4         4           4
>
```

Command: QoS Storm Unicast**Syntax:** **qos storm unicast** [enable|disable] [<packet_rate>]**Description:** Set or show the unicast storm rate limiter. The limiter will only affect flooded frames, i.e., frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.

The parameters are:

enable : Enable unicast storm control.**disable** : Disable unicast storm control.

<packet_rate>: Rate in fps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 32768k).

Example:

```
>qos storm unicast enable 4k
>qos storm unicast
Storm Unicast : Enabled      4 kfps
>
```

Command: QoS Storm Multicast**Syntax:** **qos storm multicast** [enable|disable] [<packet_rate>]**Description:** Set or show the multicast storm rate limiter. The limiter will only affect flooded frames, i.e., frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.

The parameters are:

enable : Enable multicast storm control.**disable** : Disable multicast storm control (the default).

<packet_rate>: Rate (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 32768k) in fps (frames-per-second).

Example:

```
>qos storm multicast
Storm Multicast: Disabled      1 fps
>qos storm multicast enable 4k
>qos storm multicast
Storm Multicast: Enabled       4 kfps
>
```

Command: QoS Storm Broadcast**Syntax:** **qos storm broadcast** [enable|disable] [<packet_rate>]**Description:** Set or show the broadcast storm rate limiter. The limiter will only affect flooded frames, i.e., frames with a (VLAN ID, DMAC) pair not present in the MAC Address table, where:**enable** : Enable broadcast storm control.**disable** : Disable broadcast storm control (the default).

<packet_rate>: Rate (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 32768k) in fps (frames-per-second).

Example:

```
>qos storm broadcast
Storm Broadcast: Disabled      1 fps
>qos storm broadcast enable 64k
>qos storm broadcast
Storm Broadcast: Enabled       64 kfps
>
```


Command: QoS QCL Add

Syntax: **qos qcl add** [<qce_id>] [<qce_id_next>]
 [<port_list>]
 [<tag>] [<vid>] [<pcp>] [<dei>] [<smac>] [<dmac_type>]
 [(etype [<etype>]) |
 (LLC [<DSAP>] [<SSAP>] [<control>]) |
 (SNAP [<PID>]) |
 (ipv4 [<protocol>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) |
 (ipv6 [<protocol>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])]
 [<class>] [<dp>] [<classified_dscp>]

Description: Add or modify a QoS Control Entry (QCE).
 If the QCE ID parameter <qce_id> is specified and an entry with this QCE ID already exists, the QCE will be modified. Otherwise, a new QCE will be added. If the QCE ID is not specified, the next available QCE ID will be used. If the next QCE ID parameter <qce_id_next> is specified, the QCE will be placed before this QCE in the list. If the next QCE ID is not specified and if it is a new entry added, the QCE will be placed last in the list. Otherwise if the next QCE ID is not specified and if existing QCE is modified, QCE will be in the same location in the list. To modify and move the entry to last in the list, use the word 'last' for <qce_id_next>.

Example:

```
>qos qcl add 1 last 1 tag 1 0-1 any any unicast kw1 0x900 1 any any
any k any any k any any EF yes any any k any 1 0 BE
Invalid parameter: last
```

Messages: *QCL Add failed: classified parameter missing*
Invalid parameter: last

Command: QoS QCL Delete

Syntax: **qos qcl delete** <qce_id>

Description: Delete an existing QCE entry from the QCL (QoS Control List), where:
 <qce_id>: QCE ID (1-256). The default is the next available ID.

Example:

```
>qos qcl delete 1
>qos qcl status combined

Number of QCEs: 0
>
```

Messages: *QCL Delete failed*

Command: QoS QCL Lookup

Syntax: **qos qcl lookup** [<qce_id>]

Description: Lookup a QoS Control List, where:
 <qce_id>: QCE ID (1-256), default: Next available ID.

Example:

```
>qos qcl lookup 1
>qos qcl lookup all
Invalid parameter: all

Syntax:
QoS QCL Lookup [<qce_id>]
>qos qcl lookup
Number of QCEs: 0
>
```

Command: QoS QCL status

Syntax: qos qcl status [combined|static|conflicts]

Description: Display the current QCL status (if there is any conflict in QCE for various user types).

The parameters are:

combined|static|conflicts:

combined : Shows the combined status (Static and Conflicts).

static : Shows just the static user configured status.

conflicts : Shows all conflict status.

(default : Shows the combined status)

Example 1: >qos qcl status combined

```
User          ID   Frame  Class DP DSCP      Conflict Port
-----
Static        1   Any    0     -  -        No       4-9
```

Number of QCEs: 1

>qos qcl status conflicts

Number of QCEs: 0

>qos qcl status static

```
User          ID   Frame  Class DP DSCP      Conflict Port
-----
Static        1   Any    0     -  -        No       4-9
```

Number of QCEs: 1

>

Example 2: >qos qcl status combined

```
User          ID   Frame  Class DP DSCP      Conflict Port
-----
Static        1   EType  3     0  0   (BE)    No       7-10
Static        2   Any    0     -  -        No       4-11
Static        3   Any    0     -  -        No       4-6,8-10
```

Number of QCEs: 3

>

Command: QoS QCL refresh

Syntax: qos qcl refresh

Description: This command is used to resolve QCE conflict status. Since the same hardware resource is shared by multiple applications, and it may not be available even before MAX QCE entry, this command is available to release the resource in use by other applications and use this command to acquire the resource.

Example: >qos qcl refresh

>

Mirror Commands

To debug network problems, selected traffic can be copied (mirrored) on a mirror port where a frame analyzer can be attached to analyze the frame flow. The traffic to be copied on the mirror port is selected as follows:

- All frames received on a given port (also known as ingress or source mirroring).
- All frames transmitted on a given port (also known as egress or destination mirroring).

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port (the Port to mirror). Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port.

Port mirror considerations:

- You can select more than one source port at a time, but the more ports you mirror, the less likely the mirroring port is able to handle all the traffic. So if you mirror the traffic of six heavily active ports, the destination port is likely to drop packets, providing an inaccurate mirror of the six source ports' traffic.
- The source and mirror ports must be located on the same switch.
- You can mirror the ingress or egress traffic of the source ports or both.
- While the Mirroring feature is enabled, the mirroring port is dedicated to monitoring the traffic from the source ports and can not be used for normal network operations.

These S3280 commands provide Port mirroring functions:

>**mirror ?**

Available Commands:

Mirror Configuration [<port_list>]

Mirror Port [<port>|disable]

Mirror Mode [<port_list>] [enable|disable|rx|tx]

>

The S3280 Port mirroring commands are explained below.

Command: **Show Mirror Configuration**

Syntax: **show mirror configuration** [<port_list>]

Description: Show the current mirror configuration, where:
<port_list>: Port list or 'All'. The default is 'All' ports.

Example: >**mirror config**

```
Mirror Configuration:
=====
```

```
Mirror Port: Disabled
```

```
Port  Mode
----  -
```

1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled

```
>
```

Command: **Mirror Port****Syntax:** **mirror port** [<port>|disable]**Description:** Set or show the mirror port, where:<port>**disable**: Mirror port or 'disable'. The default is 'Show' port.

Example:

```
Mirror>port 3
Mirror>port
Mirror Port: 3
Mirror>
```

Command: **Mirror Mode****Syntax:** **mirror mode** [<port_list>] [enable|disable|rx|tx]**Description:** Set or show the mirror mode, where:

<port_list>: Port list or 'all'. The default is 'All' ports.

enable : Enable Rx and Tx mirroring.**disable**: Disable Mirroring.**rx** : Enable Rx mirroring.**tx** : Enable Tx mirroring.

(default: Show mirror mode)

Example:

```
Mirror>mode 1 enable
Mirror>mode 2 enable
Mirror>mode 3 rx
Mirror>mode 4 tx
Mirror>mode

Port  Mode
----  -
1     Enabled
2     Enabled
3     Rx
4     Tx
5     Disabled
6     Disabled
7     Disabled
8     Disabled
Mirror>
```

Firmware Commands

These S3280 commands provide firmware downloads via TFTP. Note that a TFTP server must be configured and running for the **firmware load** and **firmware ipv6 load** commands to work. After the software image is uploaded, a message announces that the firmware update is initiated. After about a minute, the firmware is updated and the S3280 restarts.

You can elect to activate (swap) the image and reboot now, or activate (swap) the image manually later.

With the one-step upgrade procedure, after the software image is uploaded, a message announces that the firmware update is initiated. After about a minute, the firmware is updated and the S3280 restarts. With the two-step upgrade procedure, you can specify the “activate” parameter.

Warning: While the S3280 firmware is being updated, Web access appears to be defunct. The S3280 front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the S3280 at this time or it may fail to function afterwards.

S3280 v 1.0.3 adds support for a two-step firmware upgrade where you reboot manually at a later time. The two-step procedure is the default. You can optionally select 'Activate Image Now' to perform the one-step procedure (where the S3280 reboots automatically right away). For the two-step procedure, you first upload the firmware image and program to flash, and then manually activate the Alternate image and reboot the S3280. This procedure performs a send using a ‘simple’ interface (no completion message displays) and the S3280 is freed after use.

The S3280 firmware commands include:

>**firmware ?**

Available Commands:

Firmware Load <ip_addr_string> <file_name> [<activate>]
Firmware IPv6 Load <ipv6_server> <file_name> [<activate>]
Firmware Information
Firmware Swap
Firmware Peripheral Load <hostname> <file_name> (S3280-TST only)
Firmware Peripheral Versions (S3280-TST only)

>

Command: **Display Firmware Information**
Syntax: **firmware info**
Description: Display information about the Active and Alternate firmware images.

Example 1: >**firmware info**

```

Active Image
-----
Image       : managed
Version    : S3280 (standalone) 1.6.4
Date       : 2013-08-28T16:02:41-05:00

Alternate Image
-----
Image       : managed.bk
Version    : S3280 (standalone) 1.6.3
Date       : 2013-08-23T13:02:42-05:00

>
```

Command: Load IPv6 Firmware

Syntax: **firmware ipv6 load** <ipv6_server> <file_name>

Description: Load new firmware from a third party IPv6-capable TFTP server that is configured and running. The parameters are:

<ipv6_server>: The TFTP server's IPv6 address.

<file_name> : The name of the S3280 firmware file.

<activate> : *true*: Activate image (swap) now and reboot.

false: Activate image (swap) manually later.

Example:

```
>firmware ipv6 load ::192.0.2.1 s3280fw.dat
Download of s3280fw.dat from ::192.0.2.1 failed: Operation timed out.
>
```

Messages: *Download of S3280-v1.0.4.dat from 192.168.1.30 failed: Operation timed out.*
Download of S3280-v1.0.4.dat from 192.168.1.30 failed: Network error

You can use the firmware information command to verify the firmware load.

You must log in to the S3280 again after a successful firmware load. You can use the firmware information command to verify the firmware load.

Note: Using an IPv6 link-local address is not allowed here. Use an IPv6 Address such as **::192.0.2.1**
Do not an IPv6 Link-Local Address such as fe80::2c0:f2ff:fe00:1.

Note: The **firmware load** and **firmware ipv6 load** commands do not work with SolarWinds TFTP Server version 8.2.7 (September 2005). SolarWinds TFTP Server version 10.4.0.14 works fine for S3280 binary backups and restores.

Command: Load IPv4 Firmware

Syntax: `firmware load <ip_addr_string> <file_name>`

Description: Loads new firmware from a third-party TFTP server with the option to reboot the S3280 now or later. You must log in to the S3280 again after the reboot occurs. Note that the TFTP server must be running and properly configured. The parameters are:

<ip_addr_string>: IPv4 host address (a.b.c.d) or a host name string of the TFTP server. This TFTP server must be running and properly configured).

<file_name> : Firmware file name to download (must have a .DAT file extension). This file must be located such that the TFTP server can find it (e.g., at *C:\TFTP-Root*).

<activate> : *true*: Activate image (swap) now and reboot.

false: Activate image (swap) manually later.

```

Example: >firmware load 192.168.1.30 S3280-master.dat true
Downloaded "S3280-master.dat", 3668140 bytes
Master initiated software updating starting
Waiting for firmware update to complete
Starting flash update - do not power off device!
Erasing image...
Programming image...
... Erase from 0x40fd0000-0x40fdffff: .
... Program from 0x87ff0000-0x88000000 to 0x40fd0000: .
... Program from 0x87ff000a-0x87ff000c to 0x40fd000a: .
... Program from 0x87ff000a-0x87ff000c to 0x40fd000a: .
Restarting system...
+M25PXX : Init device with JEDEC ID 0xEF4018.
S3280 board detected (VSC7428 Rev. B).

RedBoot(tm) bootstrap and debug environment [ROMRAM]
Non-certified release, version 1_13-TN - built 19:33:13, Jun 21 2012

Copyright (C) 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008,
2009
Free Software Foundation, Inc.
RedBoot is free software, covered by the eCos license, derived from
the GNU General Public License. You are welcome to change it and/or
distribute copies of it under certain conditions. Under the license
terms, RedBoot's source code and full license terms must have been
made available to you. Redboot comes with ABSOLUTELY NO WARRANTY.

Platform: VCore-III (MIPS32 24KEc) LUTON26
RAM: 0x80000000-0x88000000 [0x800211c8-0x87fe1000 available]
FLASH: 0x40000000-0x40ffffff, 256 x 0x10000 blocks
== Executing boot script in 1.000 seconds - enter ^C to abort
RedBoot> fis load -d managed
Image loaded from 0x80040000-0x80718c60
RedBoot> go

Username:

```

If you selected **activate = true** then you must log in to the S3280 again after a successful firmware load. You can use the firmware information command to verify the firmware load.

Messages:

Downloaded "S3280-master.dat", 3612248 bytes

W firmware 00:14:45 10/firmware_check#787: Warning: Trailer: TN_PRODUCT_ID mismatch (was S3280 , want INDM1040-384-LRT)

Error: Image error

Download of ND-3284-v1.0.4.dat from 192.168.1.30 failed: File not found.

Download of INDM1040-384-LRTfw from 192.168.1.30 failed: Operation timed out.

Error: Flash is already updated with this image

Error: Image error

The maximum string length is 5.

W firmware 21:29:45 54/firmware_check#742: Warning: Trailer: TN_PRODUCT_ID mismatch (was S3280 , want INDM1040-384-LRT)

Note: You must log in to the S3280 again after a successful firmware load. You can use the firmware information command to verify the firmware load.

Note: The **firmware load** and **firmware ipv6 load** commands may not work with SolarWinds TFTP Server version 8.2.7 (September 2005). SolarWinds TFTP Server version 10.4.0.14 works fine for S3280 binary backups and restores.

Warning: While the S3280 firmware is being updated, Web access appears to be defunct. The S3280 front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the S3280 at this time or it may fail to function afterwards.

Command: **Firmware Swap**

Syntax: **firmware swap**

Description: Activate the alternate firmware image and reboot. You must log in to the S3280 again when done.

Example:

```
>firm swap
... Erase from 0x40ff0000-0x40ffffff: .
... Program from 0x87ff0000-0x88000000 to 0x40ff0000: .
... Program from 0x87ff000a-0x87ff000c to 0x40ff000a: .
Alternate image activated, now rebooting.
>+M25PXX : Init device with JEDEC ID 0xEF4018.
S3280 board detected (VSC7428 Rev. B).

RedBoot(tm) bootstrap and debug environment [ROMRAM]
Non-certified release, version 1_12-TN - built 13:45:10, Jan 26 2012

Copyright (C) 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009
Free Software Foundation, Inc.
RedBoot is free software, covered by the eCos license, derived from the
GNU General Public License. You are welcome to change it and/or distribute
copies of it under certain conditions. Under the license terms, RedBoot's
source code and full license terms must have been made available to you.
Redboot comes with ABSOLUTELY NO WARRANTY.

Platform: VCore-III (MIPS32 24KEc) LUTON26
RAM: 0x80000000-0x88000000 [0x80020ec8-0x87fe1000 available]
FLASH: 0x40000000-0x40ffffff, 256 x 0x10000 blocks
== Executing boot script in 1.000 seconds - enter ^C to abort
RedBoot> fis load -d managed
Image loaded from 0x80040000-0x806ee950
RedBoot> go

Username:
```

Messages:

Activate image (swap) now and reboot

Activate image (swap) manually later

Alternate image activated, now rebooting.

Alternate image activation failed.

Do not reset or power off the device!

E misc 00:00:00 26/pic32_spi_init_start#1594: Error: pic32_spi_read_version failed: -2

Error: Incomplete stack update - update aborted

FIRMWARE_ERROR_xxx code

Flashing, please wait...

Rebooting system...

Restarting, please wait...

Slave, only doing local update

Waiting for firmware update to complete

(Still) waiting for firmware update to complete

Warning! Device will automatically reboot. Proceed with update now?

W mirror 00:00:00 26/mirror_conf_read#335: Warning: conf_sec_open failed or size mismatch, creating defaults

W vlan 00:00:00 26/vlan_conf_read_stack#4146: Warning: version mismatch, creating defaults

Meaning: Informational or warning messages.

Recovery: 1. Wait for the message to clear. 2. Continue operation.

Command: **Firmware Peripheral Load**

Syntax: **firmware peripheral load** <hostname> <file_name>

Description: Update S3280-TST peripheral device firmware if present. **Note:** Do not reset or power off the device while it is in the process of writing the peripheral device firmware image to flash. Note that the TFTP server must be running and properly configured. The parameters are:

<**hostname**> : IP Address or Hostname of the TFTP server.

<**file_name**>: Firmware file name to be uploaded (e.g., the *HPIC32-v1.0.1.dat* file from *C:\TFTP-Root*).

```
Example: >firmware peripheral load 192.168.1.30 HPIC32-v1.0.1.dat
tftp client get failed: 9
>
>firmware peripheral load 192.168.1.30 HPIC32-v1.0.1.dat
tftp client get failed: 1
>
>firmware per load 192.168.1.30 HPIC32-v1.0.1.dat
Starting peripheral device update
Processing section 1...
Processing section 1 complete
ET-FPGA was not updated
Peripheral device update failed
>
```

ET-FPGA (External Timing FPGA) a field upgradeable chip on the External Timing board (S3280-TST only).

FPGA (field-programmable gate array) a chip that can be programmed in the field after manufacture.

PIC ("peripheral interface controller") a family of specialized microcontroller chips.

Message:

Warning: FPGA 1.1 required

Warning: FPGA 2.x required

Meaning: The S3280-TST does not automatically reboot after FPGA upgrade, but should be rebooted to ensure proper operation.

Recovery: We recommend upgrading the FPGA first, then the software, because the unit will automatically reboot after the software upgrade. If upgraded in the reverse order (main software then FPGA), you must manually reboot after the FPGA upgrade.

Message:

W firmware 00:10:29 59/handler_config_hpic_firmware#243: Warning: firmware file is too short

Meaning: You did not enter a filename for the firmware to be uploaded/upgraded.

Recovery:

1. Enter a valid filename for the firmware to be uploaded.
2. Continue operation.
3. See the "Firmware Peripheral Load" command on page 264.

Message:

Reading FPGA version failed

Reading MAC version failed

Reading MAC Swap/Loopback version failed

Reading PCS version failed

Reading Remote Update version failed

Meaning: The device upgrade failed.

Recovery:

1. Check the filename and version information.
2. See "Firmware Commands" on page 261.

Messages:

HPIC is in App mode

HPIC is in BL mode

HPIC usb data not present

illegal esce id: %lu", esce->id

invalid record: record length is odd

invalid record: record length is too long

Must explicitly add case for module ID: %d (at conf->privilege_level[i].crw = 10;

negative status code: %02X

Opening device failed\n

Peripheral Device Firmware Error

Peripheral device upgrade failed at section %d\n

Peripheral device firmware update failed

Peripheral device firmware update in progress

Processing section %d complete, please wait...

Processing section %d complete\n

Programming device, please wait...

Programming device image...\n

Programming device complete, please wait...

Programming device complete...\n

Restarting %s...\n

Restarting %s, please wait...

Starting %s flash update - do not power off device!

unexpected command in response: %02X

Updating, please wait...

%s flash update complete...\n

Writing peripheral device firmware image to flash.

Meaning: S3280-TST informational or warning messages.

Recovery:

1. Wait for the message to clear.
2. Continue operation.

Messages:

Device flash update complete...\n

Device not present

Do not reset or power off the device!

Erasing device, please wait...

Erasing %s image...

Error: Firmware file is too short

Error: Firmware file contains bad length

Error: cksum mismatch

Error: Firmware update failed

esce_id: %lu not found", esce_id

Flash crc check failed: %04X != %04X

FPGA Version: v%u.%u\n,(version.major, version.minor)

FPGA Version: Not present\n

HPIC App detected...\n

HPIC control data not present

HPIC firmware update failed

Unable to resolve DNS name

Meaning: The S3280-TST peripheral device upgrade failed.

Recovery:

1. Check the filename and version information.
2. See "[Firmware Commands](#)" on page 261.

Command: **Firmware Peripheral Versions**
Syntax: **firmware peripheral versions**
Description: Display the current version of all peripheral devices (S3280-TST only).
Example: **>firm periph ver**

```
FPGA Version: v2.1 (0x0000)
HPIC Version: Not present
ET-PIC Version: Not present
>
```

The FPGA Versions that can be reported are **FPGA Version**, **HPIC Version**, and **ET PIC Version** version.
FPGA: reports the external timing board - field programmable gate array version information.
HPIC: helper reports the programmable interrupt controller (32-bit) version information.
ET-PIC: reports the external timing board - programmable interrupt controller version information.

Messages:*tftp client get failed: 9**FPGA Version: Not present**Force to Factory mode by loading invalid user image address.**"altera_fpga_write_reg failed: %d"**Meaning:* A firmware peripheral load or version error condition exists.**Recovery:**

1. See the “Firmware Peripheral Load” command.
2. See the “Firmware Peripheral Versions” command.

Message:*Attempting load of Application Boot Address: 0x%08X\n**FPGA Running in Factory mode**User Watchdog Timer timeout**nSTATUS asserted by an external device as the result of an error**CRC error during application configuration**External configuration reset (nCONFIG) assertion**FPGA Running in Application mode**Application Boot Address: 0x%08X**FPGA Running in Application mode with Master State Machine User Watchdog Timer Enabled**Application Boot Address: 0x%08X**FPGA Running in unknown/undefined mode**User Configuration area is locked for address 0x%08X**User Configuration device id of 0x%02X does not match image of 0x%02X**User Configuration hw type of 0x%02X does not match image of 0x%02X**1166 // The exception to the rule case: S3820-TST allows for sw_function**1167 // upgrades of 1 (MACSwap Only) and/or 2 (MACSwap & 2544) in same user space.**User Configuration sw function of 0x%02X does not match image of 0x%02X**User Configuration sw function of 0x%02X is locked for image 0x%02X**Meaning:* A firmware peripheral load or version error condition exists.**Recovery:**

1. See the “Firmware Peripheral Load” command above.
2. See the “Firmware Peripheral Versions” command above.

ET-FPGA Version Compatibility Note (S3280-TST only)

The Main Firmware is pinned to the major release number of FPGA Firmware. So at a specific release of Main Firmware (e.g., v1.3.3) the required FPGA firmware should begin with with major version “1” (e.g., v1.0, v1.1, etc.). For example:

Main Firmware Version: v1.3.5
ET-FPGA Firmware Version: v1.x

This means that the ET-FPGA firmware can be released independently as long as the major version of ET-FPGA Firmware does not change. When the ET-FPGA major version is bumped, a new (compatible) version of Main Firmware will be released.

Note: It is recommended to update the FPGA firmware before updating the device firmware.

TFTP Server Messages

Message: Connection received from 192.168.1.10 on port 7700 [10/04 10:04:49.141]

Meaning: The TFTP server connected to the S328x successfully.

Message: Read request for file <S3280 -master.dat>. Mode OCTET [10/04 10:04:49.141]

Using local port 1947 [10/04 10:04:49.157]

<S3280 -master.dat>: sent 7056 blks, 3612248 bytes in 3 s. 0 blk resent [10/04 10:04:52.829]

Connection received from 192.168.1.10 on port 7701 [10/04 10:08:44.427]

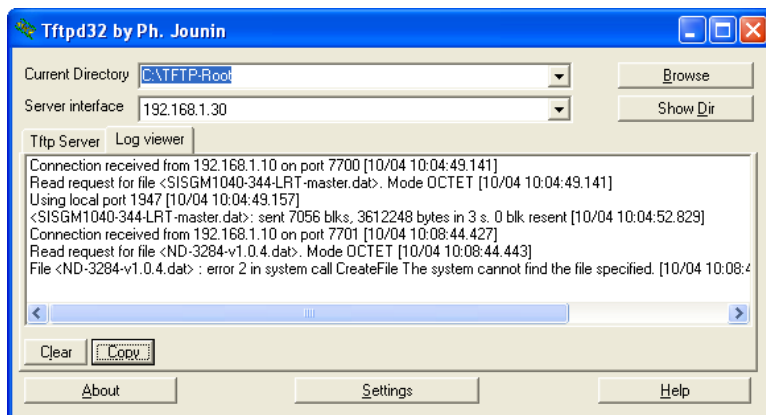
Meaning: The TFTP server transferred the file to the S328x successfully.

Message: Read request for file <ND-3284-v1.0.4.dat>. Mode OCTET [10/04 10:08:44.443]

File <ND-3284-v1.0.4.dat> : error 2 in system call CreateFile The system cannot find the file specified. [10/04 10:08:44.443]

Meaning: The TFTP server failed to transfer the file to the S3280.

Example:



Recovery:

1. Make sure the TFTP Server "Current Directory" points to C:\TFTP-Root.
2. Make sure that you have specified the correct file (xxxxxxx.DAT).
3. See "[Firmware Commands](#)" on page 261.

PTP Commands

PTP (Precision Time Protocol) is a network protocol for synchronizing the clocks of computer systems. PTP defines a procedure allowing many spatially distributed real-time clocks to be synchronized through a "package-compatible" network (normally Ethernet). Note that PTP configuration of the S3280 MGMT port is not supported.

PTP knows various types of clocks, and acts as a master-to-slave protocol. A clock in an end device is known as an "Ordinary" clock, and a clock in a transmission component like an Ethernet switch is a "Boundary" clock (BC) or "Transparent" clock (TC). A "Master" synchronizes the respective slaves connected to it. The synchronization process is divided into two phases. First the time difference between the master and the slave is corrected; this is the offset correction. With IEEE1588-2008, two modes are known for the synchronization process: two-step-mode and one-step-mode. The second phase of the synchronization, delay measurement, determines the run time between slave and master. It is determined by the "Delay Request" and "Delay Response" messages in a similar way, and the clocks adjusted accordingly. This can also be done in one-step or in two-step mode. Boundary clocks are required wherever there is a change of the communication technology or other network elements block the propagation of the PTP messages. The IEEE1588-2008 standard knows two types of transparent clocks: End-to-End (E2E) and Peer-to-Peer (P2P). See the IEEE Standards web site at <http://ieeexplore.ieee.org/xpl/standards.jsp> for current editions and amendments.

Note: at S3280 v 1.0.2, PTP is available over Ethernet and IPv4 only. PTP under IPv6 will be supported at a future release. **Note:** you must have a PTP clock instance configured for accurate RFC 2544 Latency test step timestamps.

These S3280 commands provide IEEE 1588 Precision Time Protocol (PTP) functions:

>ptp ?

Available Commands:

```

PTP Configuration <clockinst>
PTP PortState <clockinst> [<port_list>] [enable|disable|internal]
PTP ClockCreate <clockinst> [<devtype>] [<twostep>] [<protocol>] [<oneway>] [<clockid>] [<tag_enable>] [<vid>] [<prio>]
PTP ClockDelete <clockinst> [<devtype>]
PTP DefaultDS <clockinst> [<priority1>] [<priority2>] [<domain>]
PTP CurrentDS <clockinst>
PTP ParentDS <clockinst>
PTP Timingproperties <clockinst> [<utcoffset>] [<valid>] [<leap59>] [<leap61>] [<timetrac>] [<freqtrac>] [<ptptimescale>]
  [<timesource>]
PTP PortDataSet <clockinst> [<port_list>] [<announceintv>] [<announceto>] [<syncintv>] [<delaymech>]
  [<minpdelayreqintv>] [<delayasymmetry>] [<ingressLatency>] [<egressLatency>]
PTP LocalClock <clockinst> [update|show|ratio] [<clockratio>]
PTP Filter <clockinst> [<def_delay_filt>] [<period>] [<dist>]
PTP Servo <clockinst> [<displaystates>] [<ap_enable>] [<ai_enable>] [<ad_enable>] [<ap>] [<ai>] [<ad>]
PTP SlaveTableUnicast <clockinst>
PTP UniConfig <clockinst> [<index>] [<duration>] [<ip_addr>]
PTP ForeignMasters <clockinst> [<port_list>]
PTP EgressLatency [show|clear]
PTP MasterTableUnicast <clockinst>
PTP ExtClock Output Mode [<ext_clock_enable>] [<clockfreq_out>]
PTP ExtClock Input Mode [<ext_clock_enable>] [<clockfreq_in>]
PTP ExtClock Impedance [<impedance>]
PTP ExtClock Input Status [<clear>]
PTP Wireless mode <clockinst> [<port_list>] [enable|disable]
PTP Wireless pre notification <clockinst> <port_list>
PTP Wireless delay <clockinst> [<port_list>] [<base_delay>] [<incr_delay>]
>

```

The S3280 PTP commands are explained below.

Command: PTP Configuration

Syntax: ptp configuration [<clockinst>]

Description: Show all current PTP Clock configuration and status.

Example:

```
>ptp config

PTP Configuration:
=====

PTP Clock Config, Clock instance 0
*****

Clock Default Data Set:
ClockId  DeviceType  2StepFlag  Ports  ClockIdentity  Dom
-----  -
0         Ord-Bound    True       10     00:c0:f2:ff:fe:21:b8:c4  0

ClockQuality          Pri1  Pri2
-----
Cl:251 Ac:Unknwn Va:65535  128  128

Protocol  One-Way  VLAN Tag Enable  VID  PCP
-----
Ethernet  False    True             0    0

Clock Current Data Set:
stpRm  OffsetFromMaster  MeanPathDelay
-----
0      0.000,000,000  0.000,000,000

Clock Parent Data Set:
ParentPortIdentity  port  Pstat  Var  ChangeRate
-----
00:c0:f2:ff:fe:21:b8:c4  0     False  0    0

GrandmasterIdentity  GrandmasterClockQuality  Pri1  Pri2
-----
00:c0:f2:ff:fe:21:b8:c4  Cl:251 Ac:Unknwn Va:65535  128  128

Clock Time Properties Data Set:
UtcOffset  Valid  leap59  leap61  TimeTrac  FreqTrac  ptpTimeScale  TimeSource
-----
0          False  False   False   False     False     True           160

Servo parameters:
Display  P-enable  I-enable  D-enable  'P'constant  'I'constant  'D'constant
-----
False   True     True     True     3            80           40

Filter parameters:
DelayFilter  period  dist
-----
6           1       2

Unicast Slave Configuration:
index  duration  ip_address  grant  CommState
-----
0      100      0.0.0.0    0      IDLE
1      100      0.0.0.0    0      IDLE
2      100      0.0.0.0    0      IDLE
3      100      0.0.0.0    0      IDLE
4      100      0.0.0.0    0      IDLE

Port Data Set(s):
```



```

Port  Stat  MDR  PeerMeanPathDel  Anv  ATo  Syv  Dlm  MPR  DelayAsymmetry  Ingr
essLatency  EgressLatency  Ver
----  ----  ---  -
2      dsbl  0    0.000,000,000  1    3    0    e2e  3    0.000,000,000  0.0
00,000,000  0.000,000,000  2
3      dsbl  0    0.000,000,000  1    3    0    e2e  3    0.000,000,000  0.0
00,000,000  0.000,000,000  2

Local Clock Current Time:PTP Time (0)      : 1970-01-05T01:41:28+00:00 542,359,260
Clock Adjustment method: Internal Timer
>

```

Messages: *Clock instance 1 : does not exist or timestamp feature not available*

Command: **PTP Port State**

Syntax: **ptp portstate** <clockinst> [<port_list>] [enable|disable|internal]

Description: Set or show the PTP port state. Note that PTP configuration of the S3280 MGMT port is not supported. The parameters are:

 <**clockinst**>: The clock instance number (0-3).

 <**port_list**>: Port list or 'All'. The default is 'All' ports.

enable : Enable PTP port.

disable : Disable PTP port.

internal : Enable PTP port as internal (in a distributed environment).

(The default is 'Show actual port state'.)

Example:

```

>ptp portstate 0
Port  PTP-State  Internal  Link  Port-Timer  Vlan-forw  Phy-timestamper
----  -
2  dsbl      FALSE    Down  In Sync     Discard     FALSE
>

```

Messages: *Clock instance 1 : does not exist*
 Clock instance 1 : does not exist or timestamp feature not available

Command: PTP Port Data Set

Syntax: **ptp portdataset** <clockinst> [<port_list>] [<announceintv>] [<announceto>] [<syncintv>]
 [<delaymech>] [<minpdelayreqintv>] [<delayasymmetry>] [<ingresslatency>]
 [<egresslatency>]

Description: Set or show PTP port data set, where:

- <**clockinst**> : clock instance number [0..3].
- <**port_list**> : Port list or 'All'. The default is 'All' ports.
- <**announceintv**> : [-3..4] Log2 of mean announce interval in seconds.
- <**announceto**> : [-1..10] Log2 of announce receipt timeout in seconds.
- <**syncintv**> : [-7..4] Log2 of sync interval in seconds.
- <**delaymech**> : The 'delaymech' parameter takes the following values:
 - e2e : The port is configured to use the delay request-response mechanism.
 - p2p : The port is configured to use the peer delay mechanism.
- <**minpdelayreqintv**>: [-7..5] Log2 of min delay req interval in seconds.
- <**delayasymmetry**> : path delay asymmetry measured in ns (nano seconds).
- <**ingresslatency**> : ingress latency measured in ns (nano seconds).
- <**egresslatency**> : egress latency measured in ns (nano seconds).

Example 1:

```
>ptp portdataset 1 1 1 1 1 e2e 2 10 10 10
>ptp portdataset 1
Port Stat MDR PeerMeanPathDel Anv ATo Syv Dlm MPR DelayAsymmetry Ingr
essLatency EgressLatency Ver
-----
1 mstr 3 0.000,000,000 1 3 0 e2e 3 0.000,000,000 0.0
00,000,000 0.000,000,000 2
>
```

Example 2:

```
>ptp portdataset 1 1 1 1 1 e2e 2 10 10 10
>ptp portdataset 1
Port Stat MDR PeerMeanPathDel Anv ATo Syv Dlm MPR DelayAsymmetry IngressLatency EgressLatency Ver
-----
1 mstr 3 0.000,000,000 1 3 0 e2e 3 0.000,000,000 0.0 00,000,000
0.000,000,000 2
>
```

Messages: *Clock instance 1 : does not exist*

Note: you must have a PTP clock instance configured for accurate RFC 2544 Latency test step timestamps. PTP must be running on both devices to synchronize the Time of Day.

Command: PTP Clock Create

Syntax: **ptp clockcreate** <clockinst> [<devtype>] [<twostep>] [<protocol>] [<oneway>] [<clockid>] [<tag_enable>] [<vid>] [<prio>]

Description: Create or show a PTP clock instance data, where:

<**clockinst**> : The clock instance number [0..3]. A maximum of four clock instances can exist.

<**devtype**> : The ‘devtype’ parameter takes the following values:

- ord : Ordinary/Boundary clock.
- p2p : Peer-to-peer transparent clock.
- e2e : End-to-end transparent clock.
- mst : Master only clock.
- slv : Slave only clock.

(The default is ‘Show actual init parameters’.)

<**twostep**> : The ‘twostep’ parameter takes the following values:

- true : Follow-up messages are used.
- false : No follow-up messages are used.

<**protocol**> : The protocol parameter takes the following values:

- ethernet : The clock uses multicast Ethernet protocol.
- ip4multi : The clock uses IPv4 multicast protocol.
- ip4uni : The clock uses IPv4 unicast protocol.

Note : IPv4 unicast protocol only works in Master only and Slave only clocks.

See parameter <devtype>.

In a unicast Slave only clock you must also configure which master clocks to request Announce and Sync messages from. See the ‘UniConfig’ command.

<**oneway**> : The oneway parameter takes the following values:

- true : The clock slave uses one-way measurements, i.e., no delay requests.
- false : The clock slave uses two-way measurements.

<**clockid**> : 8 byte clock identity (xx:xx:xx:xx:xx:xx:xx:xx).

<**tag_enable**>: The ‘tag_enable’ parameter takes the following values:

- true : The ptp frames are tagged with the VLAN tag specified in the VID field.
Note : Packets are only tagged if the port is configured for vlan tagging, i.e.,: Port Type != Unaware and PortVLAN mode == None.
- false : The ptp frames are sent untagged.

<**vid**> : The VID parameter takes the following values:

- 0 - 4094 : The range of VIDs ptp can use to send tagged frames.

<**prio**> : The Prio parameter takes the following values:

- 0 - 7 : The range of Priorities ptp can use in the tagged frames.

Example:

```
>ptp clockcreate 0
ClockId DeviceType 2StepFlag Ports ClockIdentity Dom
-----
0 Inactive
>ptp clockcreate 1
ClockId DeviceType 2StepFlag Ports ClockIdentity Dom
-----
1 Ord-Bound False 10 00:c0:f2:ff:fe:21:b8:c4 1

ClockQuality Pri1 Pri2
-----
Cl:251 Ac:Unknwn Va:65535 128 128

Protocol One-Way VLAN Tag Enable VID PCP
-----
Ethernet False False 0 0
```

```
>ptp clockcreate 2
ClockId DeviceType 2StepFlag Ports ClockIdentity Dom
-----
2 P2pTransp False 10 00:c0:f2:ff:fe:21:b8:c4 2

ClockQuality Pri1 Pri2
-----
Cl:251 Ac:Unknwn Va:65535 128 128

Protocol One-Way VLAN Tag Enable VID PCP
-----
Ethernet False False 0 0
>
```

Messages: **Cannot create clock instance 1 : a Ord-Bound clock type already exists**
Missing <clockinst> parameter

Command: **PTP Clock Delete**

Syntax: **ptp clockdelete <clockinst> [<devtype>]**

Description: Delete an existing PTP clock instance, where:

<clockinst>: clock instance number (0-3).

<devtype> : The devtype parameter takes the following values:

- ord** : Ordinary/Boundary clock
- p2p** : Peer-to-peer transparent clock
- e2e** : End-to-end transparent clock
- mst** : Master only clock
- slv** : Slave only clock

(The default is 'Show actual init parameters'.)

Example: >ptp clockdelete 1

```
ClockId DeviceType 2StepFlag Ports ClockIdentity Dom
-----
1 Ord-Bound False 9 00:c0:f2:ff:fe:00:00:01 1

ClockQuality Pri1 Pri2
-----
Cl:251 Ac:254 Va:65535 128 128

Protocol One-Way VLAN Tag Enable VID PCP
-----
Ethernet False False 0 0
>
```

Command: PTP Default DS**Syntax:** **ptp defaultds** <clockinst> [<priority1>] [<priority2>] [<domain>]**Description:** Set or show PTP clock Default Data Set priority1 and priority2 as used in the best master clock algorithm. The lower values take precedence. The parameters are:<**clockinst**>: clock instance number [0..3].<**priority1**>: [0..255] Clock priority 1 for PTP BMC algorithm.<**priority2**>: [0..255] Clock Priority 2 for PTP BMC algorithm.<**domain**> : [0..127] PTP clock domain id (0 = default) for PTP.**Example:**

```
>ptp defaultds 1 5 25 0
>ptp defaultds 1
ClockId DeviceType 2StepFlag Ports ClockIdentity Dom
-----
1 Ord-Bound False 10 00:c0:f2:ff:fe:00:00:01 0

ClockQuality Pri1 Pri2
-----
Cl:251 Ac:254 Va:65535 5 25

Protocol One-Way VLAN Tag Enable VID PCP
-----
Ethernet False False 0 0
>
```

Command: PTP Current DS**Syntax:** **ptp currentds** <clockinst>**Description:** Show PTP clock Current Data set, where:<**clockinst**>: clock instance number (0-3).**Example:**

```
>ptp currentds 1
stpRm OffsetFromMaster MeanPathDelay
-----
0 0.000,000,000 0.000,000,000
>
```

Command: PTP Parent DS**Syntax:** **ptp parentds** <clockinst>**Description:** Show PTP clock Parent Data set, where:<**clockinst**>: clock instance number (0-3).**Example:**

```
>ptp parentds 1
ParentPortIdentity port Pstat Var ChangeRate
-----
00:c0:f2:ff:fe:00:00:01 0 False 0 0

GrandmasterIdentity GrandmasterClockQuality Pri1 Pri2
-----
00:c0:f2:ff:fe:00:00:01 Cl:251 Ac:254 Va:65535 5 25
>
```

Command: PTP Timing Properties

Syntax: **ptp timingproperties** <clockinst> [<utcoffset>] [<valid>] [<leap59>] [<leap61>] [<timetrac>] [<freqtrac>] [<ptptimescale>] [<timesource>]

Description: Set or show existing PTP clock Timing properties Data set. The parameters are:

- <**clockinst**> : clock instance number [0..3]
- <**utcoffset**> : PTP clock offset between UTC and TAI in seconds.
- <**valid**> : The offset 'valid' parameter takes the following values:
 - false : The UTC offset is not valid.
 - true : The UTC offset is valid.
- <**leap59**> : The leap59 parameter takes the following values:
 - false : no leap59 in current day.
 - true : last minute of current day contains 59 sec.
- <**leap61**> : The leap61 parameter takes the following values:
 - false : no leap61 in current day.
 - true : last minute of current day contains 61 sec.
- <**timetrac**> : The timetraceable parameter takes the following values:
 - false : timing is not traceable.
 - true : timing is traceable..
- <**freqtrac**> : The freqtraceable parameter takes the following values:
 - false : frequency is not traceable.
 - true : frequency is traceable.
- <**ptptimescale**>: The timescale parameter takes the following values:
 - false : timing is not a PTP time scale
 - true : timing is a PTP time scale.
- <**timesource**> : [0..255] Time source (160 = internal oscillator). Values include:
 - 16** (0x10) ATOMIC_CLOCK
 - 32** (0x20) GPS
 - 48** (0x30) TERRESTRIAL_RADIO
 - 64** (0x40) PTP
 - 80** (0x50) NTP
 - 96** (0x60) HAND_SET
 - 144** (0x90) OTHER
 - 160** (0xA0) INTERNAL_OSCILLATOR

Example:

```
>ptp timingproperties 0 60 true false false false false false 160
>ptp timingproperties 0
-----
UtcOffset  Valid  leap59  leap61  TimeTrac  FreqTrac  ptpTimeScale  TimeSource
-----
60         True   False   False   False     False     False         160
>
```

Command: PTP Port DataSet

Syntax: **ptp portdataset** <clockinst> [<port_list>] [<announceintv>] [<announceto>] [<syncintv>] [<delaymech>] [<minpdelayreqintv>] [<delayasymmetry>] [<ingressLatency>] [<egressLatency>]

Description: Set or show PTP port data set, where:

- <clockinst> : clock instance number [0..3]
- <port_list> : Port list or 'all', default: All ports.
- <announceintv> : [-3..4] Log2 of mean announce interval in seconds.
- <announceto> : [-1..10] Log2 of announce receipt timeout in seconds.
- <syncintv> : [-7..4] Log2 of sync interval in seconds.
- <delaymech> : The delaymech parameter takes the following values:
 - e2e: The port is configured to use the delay request-response mechanism
 - p2p: The port is configured to use the peer delay mechanism
- <minpdelayreqintv>: [-7..5] Log2 of minimum delay required interval in seconds.
- <delayasymmetry> : path delay asymmetry measured in ns (nano seconds).
- <ingresslatency> : ingress latency measured in ns (nano seconds).
- <egresslatency> : egress latency measured in ns (nano seconds).

Example:

```
>ptp portdataset 1 1 1 1 1 e2e 1 10 10 10
>ptp portdataset 1
Port Stat MDR PeerMeanPathDel Anv ATo Syv Dlm MPR DelayAsymmetry IngressLatency
EgressLatency Ver
-----
-----
>
```

Note: you must have a PTP clock instance configured for accurate RFC 2544 Latency test step timestamps. PTP must be running on both devices to synchronize the Time of Day.

Command: PTP Local Clock

Syntax: **ptp localclock** <clockinst> [update|show|ratio] [<clockratio>]

Description: Update or show PTP current time, or set master clock ratio, where:

- <clockinst> : clock instance number (0-3).
- update|show|ratio:** PTP local clock:
 - update** : The local clock is synchronized to the eCos system clock.
 - show** : The local clock current time is shown.
 - ratio** : Set the local master clock frequency ratio in units of 0,1 PPB (ratio > 0 => faster clock, ratio < 0 => slower clock).
- <clockratio> : [-10.000.000..+10.000.000] Clock frequency ratio in 0,1 PPB.

Example:

```
>ptp localclock 1 show 100
PTP Time (1) : 1970-01-04T03:08:58+00:00 576,423,480
Clock Adjustment method: Software
>ptp localclock 0 update
>ptp localclock 0
PTP Time (0) : 1970-01-01T00:43:24+00:00 888,389,556
Clock Adjustment method: Internal Timer
>ptp localclock 0 show
PTP Time (0) : 1970-01-01T00:47:07+00:00 348,600,876
Clock Adjustment method: Internal Timer
>ptp localclock 0 ratio -5
>ptp localclock 0 show
PTP Time (0) : 1970-01-01T00:48:07+00:00 149,773,276
Clock Adjustment method: Internal Timer
>
```

Command: PTP Filter**Syntax:** `ptp filter <clockinst> [<def_delay_filt>] [<period>] [<dist>]`**Description:** Set or show PTP clock filter data, where:`<clockinst>` : clock instance number [0..3]`<def_delay_filt>`: [1..6] Log2 of timeconstant in delay filter.`<period>` : [1..1000] Measurement period in number of sync events. **Note:** In configurations with Timestamp enabled PHYs, the period is automatically increased, if $(\text{period} * \text{dist} < \text{SyncPackets pr sec}/4)$, i.e., a maximum of 4 adjustments are made per second.`<dist>` : [1..10] Distance between servo update n number of measurement periods:

If Distance is 1 the offset is averaged over the 'period',

If Distance is >1 the offset is calculated using 'min' offset.

Example:

```
>ptp filter 1 3 50 3
>ptp filter 1
DelayFilter  period  dist
-----
3           50      3
>
```

Command: PTP Servo**Syntax:** `ptp servo <clockinst> [<displaystates>] [<ap_enable>] [<ai_enable>] [<ad_enable>] [<ap>] [<ai>] [<ad>]`**Description:** Set or show PTP clock servo data. The default clock servo uses a PID regulator to calculate the current clock rate:

$$\text{clockAdjustment} = \text{OffsetFromMaster} / \text{P constant} + \text{Integral}(\text{OffsetFromMaster}) / \text{I constant} + \text{Differential}(\text{OffsetFromMaster}) / \text{D constant}$$

The **P**roportional-**I**ntegral-**D**erivative controller (PID controller) is a control loop feedback mechanism (controller) used in industrial control systems as a feedback controller. The PID controller calculates an "error" value as the difference between a measured process variable and a desired setpoint. The PID controller tries to minimize the error by adjusting the process control inputs.

The PID controller calculation involves three separate constant parameters: the Proportional, the Integral, and the Derivative values (denoted P, I, and D). These values can be interpreted in terms of time, where: **P** depends on the present error, **I** on the accumulation of past errors, and **D** is a prediction of future errors, based on current rate of change. The parameters are:

`<clockinst>` : clock instance number (0-3).`<displaystates>`: The 'displaystates' parameter takes the following values:

true : Display clock state and measurements.

false : Do not display clock state and measurements.

`<ap_enable>` : true : Enable the 'P' component in the regulator.

false : Disable the 'P' component in the regulator.

`<ai_enable>` : true : Enable the 'I' component in the regulator.

false : Disable the 'I' component in the regulator.

`<ad_enable>` : true : Enable the 'D' component in the regulator.

false : Disable the 'D' component in the regulator.

`<ap>` : [1..1000] 'P' component in the regulator.`<ai>` : [1..10000] 'I' component in the regulator.`<ad>` : [1..10000] 'D' component in the regulator.

Example:

```

>ptp servo 1
Display P-enable I-enable D-enable 'P'constant 'I'constant 'D'constant
-----
False   True     True     True     3         80        40
>ptp servo 1 true true true false
>ptp servo 1
Display P-enable I-enable D-enable 'P'constant 'I'constant 'D'constant
-----
True    True     True     False    0         0         0
>ptp servo 2
Display P-enable I-enable D-enable 'P'constant 'I'constant 'D'constant
-----
False   True     True     True     3         80        40
>ptp servo 3
Display P-enable I-enable D-enable 'P'constant 'I'constant 'D'constant
-----
False   True     True     True     3         80        40
>ptp servo 4
Invalid <clockinst> parameter: 4

```

Command: **PTP Slave Table Unicast***Syntax:* **ptp slavetableunicast** <clockinst>*Description:* Show the Unicast slave table of the requested unicast masters, where:
<clockinst>: clock instance number [0..3].*Example:*

```

>ptp slavetableunicast 1
ip_addr      stat   mac_addr    port   sourceportidentity   grant
-----
>

```

Command: **PTP UniConfig***Syntax:* **ptp uniconfig** <clockinst> [<index>] [<duration>] [<ip_addr>]*Description:* Set or show the Unicast Slave configuration, where:
<clockinst>: clock instance number [0..3].
<index> : [0..4] Index in the slave table.
<duration> : [10..1000] Number of seconds for which the Announce/Sync messages are requested.
<ip_addr> : IPv4 address of requested master clock.*Example:*

```

>ptp uniconfig 1 1 30 192.168.1.30
>ptp uniconfig 1
index  duration  ip_address  grant  CommState
-----
0      100       0.0.0.0    0      IDLE
1      30        192.168.1.30  0      IDLE
2      100       0.0.0.0    0      IDLE
3      100       0.0.0.0    0      IDLE
4      100       0.0.0.0    0      IDLE
>

```

Command: PTP Foreign Masters

Syntax: `ptp foreignmasters <clockinst> [<port_list>]`

Description: Show PTP port foreign masters data set, where:
 <clockinst>: clock instance number [0..3].
 <port_list>: Port list or 'All'. The default is 'All' ports.

Example:

```
>ptp foreignmasters 1 all
Port ForeignmasterIdentity ForeignmasterClockQuality Pri1 Pri2 Qualif Best
-----
>
```

Command: PTP Egress Latency

Syntax: `ptp egresslatency [show|clear]`

Description: Show or clear the One-step egress latency observed in systems where the time stamping is done in software. The parameters are:

show|clear: PTP Ingress latency, either:

show : Show the observed Egress latency, or

clear : Clear the observed Egress latency.

Example:

```
>ptp egresslatency show
min mean max count
-----
0.000,000,000 0.000,000,000 0.000,000,000 0
>ptp egresslatency clear
Observed Egress Latency counters cleared
```

Command: PTP Master Table Unicast

Syntax: `ptp mastertableunicast <clockinst>`

Description: Show the Unicast master table of the slaves that have requested unicast communication, where:
 <clockinst>: clock instance number [0-3].

Example:

```
>ptp mastertableunicast 1
ip_addr mac_addr port Ann Sync
-----
>
```

Command: PTP ExtClock Output Mode

Syntax: `ptp extClock output mode` [<ext_clock_enable>] [<clockfreq_out>]

Description: Update or show the IEEE 1588 SMB Output, where:

<ext_clock_enable>:

enable : Enable the external SMB.

disable : Disable the external SMB.

<clockfreq_out> : External clock output frequency (1 - 25000000 Hz).

Example:

```
>ptp extClock output mode
PTP ExtClock Output Mode: State: Enabled, Frequency: 1 Hz
>ptp extClock output mode enable 80000
>ptp extClock output mode
PTP ExtClock Output Mode: State: Enabled, Frequency: 80000 Hz
>
```

Command: PTP ExtClock Input Mode

Syntax: `ptp extClock Input Mode` [<ext_clock_enable>] [<clockfreq_in>]

Description: Update or show the IEEE 1588 SMB Input, where:

<ext_clock_enable>:

enable : Enable the external SMB.

disable : Disable the external SMB.

<clockfreq_in> : External clock input frequency, either:

[1PPS|8KHz|64KHz|1.544MHz|2.048MHz|10MHz|19.44MHz|25MHz]

Example:

```
>ptp extclock input mode
PTP ExtClock Input Mode: State: Enabled, Frequency: 64 KHz
>ptp extclock input mode enable 8KHz
>ptp extclock input mode
PTP ExtClock Input Mode: State: Enabled, Frequency: 8 KHz
>ptp extclock input mode 25MHz
>ptp extclock input mode
PTP ExtClock Input Mode: State: Disabled, Frequency: 25 MHz
>
```

Command: PTP ExtClock Impedance

Syntax: `ptp extclock impedance` [<impedance>]

Description: Update or show External I/O Impedance, where:

<impedance>:

50 : 50 ohm external I.O impedance.

75 : 75 ohm external I.O impedance.

Hi-Z : not impedance termination driven, "tri-stated" or "floating".

Example:

```
>ptp extclock impedance
PTP ExtClock Impedance: 50 Ohms
>ptp extclock imp 75
>ptp extclock imp
PTP ExtClock Impedance: 75 Ohms
>ptp extclock imp Hi-Z
>ptp extclock imp
PTP ExtClock Impedance: Hi-Z
>
```

Command: **PTP ExtClock Input Status**
Syntax: **ptp extClock input status** [<clear>]
Description: Show current IEEE 1588 Input status, where:
<clear> : Clear (reset to zero) statistics.

Example:

```
>ptp extclock input status
IEEE 1588 Input Status:

Input Frequency: 0
Input 1PPS Offset: 2147483647
Input 1PPS Status: Invalid

MTC Signal Status: Invalid
MTC Offset Min: 2147483647
MTC Offset Max: -2147483647
MTC Offset Mean: 0
MTC Offset Current: 2147483647
>
```

Messages:

External Clock feature not present

External PPS feature not present

Frequency must be an integer value between 2 kHz and 25 MHz

One PPS and External Clock feature not present

PTP External One PPS mode: %s, frequency : %ld\n

PTP External One PPS mode: %s, frequency : %ld, VCXO

This browser doesn't support dynamic tables.

Command: PTP Wireless Mode

Syntax: **ptp wireless mode** <clockinst> [<port_list>] [enable|disable]

Description: Show or set the wireless mode (this mode is only valid for 2-step BC), where:

<clockinst>: clock instance number (0-3).

<port_list>: Port list or 'all', default: All ports.

enable : Enable port Wireless mode.

disable : Disable port Wireless mode.

(The default is 'Show actual port state'.)

Example:

```
>ptp wireless mode 1
Port Wireless Mode
-----
>ptp wireless mode 0
Port Wireless Mode
-----
>ptp wireless mode 2
Port Wireless Mode
-----
>ptp wireless mode 0
Port Wireless Mode
-----
1 Disabled
2 Disabled
3 Disabled
4 Disabled
5 Disabled
6 Disabled
7 Disabled
8 Disabled
9 Disabled
10 Disabled
>ptp wireless mode 0 4,5 enable
Port Wireless Mode
-----
4 Enabled
5 Enabled
>
```

Messages: *Missing <clockinst> parameter*
wireless mode not available for ptp instance 0, port 6

Command: PTP Wireless Pre Notification**Syntax:** **ptp wireless pre notification** <clockinst> <port_list>**Description:** Set the wireless delay change pre-notification. This command is only valid if wireless mode is enabled. The parameters are:<**clockinst**>: clock instance number (0-3).<**port_list**>: Port list or 'all'. The default is 'All' ports.**Example:**

```

>ptp wireless pre notif 1
>ptp wireless pre notif 1 1
>ptp wireless pre notif 0 all
Wireless pre notification set for ptp instance 0, port 1
Wireless pre notification set for ptp instance 0, port 2
Wireless pre notification set for ptp instance 0, port 3
Wireless pre notification set for ptp instance 0, port 4
Wireless pre notification set for ptp instance 0, port 5
Wireless pre notification set for ptp instance 0, port 6
Wireless pre notification set for ptp instance 0, port 7
Wireless pre notification set for ptp instance 0, port 8
>

```

Messages:*Missing <port_list> parameter**Wireless mode not available for ptp instance 1, port 1***Command: PTP Wireless Delay****Syntax:** **ptp wireless delay** <clockinst> [<port_list>] [<base_delay>] [<incr_delay>]**Description:** Show or set the wireless delay, where:<**clockinst**> : clock instance number (0-3).<**port_list**> : Port list or 'All'. The default is 'All' ports.<**base_delay**>: [0 - 1,000,000,000] Base wireless transmission delay (in nano seconds).<**incr_delay**>: [0 - 1,000,000] Incremental wireless transmission delay per byte (in nano seconds).**Example:**

```

>ptp wireless delay 1
Port   Wireless Mode   Base_delay(ns)   Incr_delay(ns)
-----
>ptp wireless delay 0
Port   Wireless Mode   Base_delay(ns)   Incr_delay(ns)
-----
  1   Disabled           0.000           0.000
  2   Disabled           0.000           0.000
  3   Disabled           0.000           0.000
  4   Enabled            0.000           0.000
  5   Enabled            0.000           0.000
  6   Disabled           0.000           0.000
  7   Disabled           0.000           0.000
  8   Disabled           0.000           0.000
  9   Disabled           0.000           0.000
 10   Disabled           0.000           0.000
>

```

Messages:*Missing <clockinst> parameter**Wireless mode not available for ptp instance x, port y*

PTP Parameters:

Clock Frequency - This lets you set the Clock Frequency. The valid values are 1 - 25000000 Hz (1 - 25MHz).

PTP Clock Configuration

Delete - Check this box and click on 'Save' to delete the clock instance.

Clock Instance - Indicates the Instance of a particular Clock Instance [0..3]. Enter a Clock Instance number to set (define) the Clock details.

Device Type - Indicates the Type of the Clock Instance. There are five Device Types.

1. Ord-Bound - clock's Device Type is Ordinary-Boundary Clock.
2. P2p Transp - clock's Device Type is Peer to Peer Transparent Clock.
3. E2e Transp - clock's Device Type is End to End Transparent Clock.
4. MastrOnly - clock's Device Type is Master Only.
5. SlaveOnly - clock's Device Type is Slave Only.

Clock Adjustment method: Software, Internal Timer, or External Timing Board.

Port List

Set check mark for each port configured for this Clock Instance.

2 Step Flag - Static member: defined by the system, true if two-step Sync events and Pdelay_Resp events are used .

Clock Identity - shows unique clock identifier.

One Way - If true, one way measurements are used. This parameter applies only to a slave. In oneway mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.

Protocol - Transport protocol used by the PTP protocol engine, either:

- * ethernet PTP over Ethernet multicast
- * ip4multi PTP over IPv4 multicast
- * ip4uni PTP over IPv4 unicast

Note: IPv4 unicast protocol only works in Master only and Slave only clocks. See the 'Device Type' parameter. In a unicast Slave only clock, you must also configure which master clocks to request Announce and Sync messages from. See "Unicast Slave Configuration".

VLAN Tag Enable - Enables the VLAN tagging for the PTP frames.

Note: Packets are only tagged if the port is configured for VLAN tagging (i.e., Port Type != Unaware and PortVLAN mode == None).

VID - VLAN Identifier used for tagging the PTP frames.

PCP - Priority Code Point value used for PTP frames.

MVR Commands

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP) networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs. The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested them.

The MVR feature enables multicast traffic forwarding on the Multicast VLANs. In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports. MVR can create up to eight MVR VLANs with corresponding channel settings for each Multicast VLAN. Up to 256 group addresses for channel settings can exist.

The available MVR commands are:

```
>mvr ?
```

Available Commands:

MVR Configuration

MVR Mode [enable|disable]

MVR VLAN Setup [<mvid>] [add|del|upd] [(Name <mvr_name>)]

MVR VLAN Mode [<vid>|<mvr_name>] [dynamic|compatible]

MVR VLAN Port [<vid>|<mvr_name>] [<port_list>] [source|receiver|inactive]

MVR VLAN LLQI [<vid>|<mvr_name>] [mvr_param_llqi]

MVR VLAN Channel [<vid>|<mvr_name>] [add|del|upd] [channel] [channel_bound] [(Name <grp_name>)]

MVR VLAN Priority [<vid>|<mvr_name>] [priority] [tagged|untagged]

MVR Immediate Leave [<port_list>] [enable|disable]

MVR Status [<vid>] [clear]

MVR Groups [<vid>]

MVR SFM [<vid>] [<port_list>]

```
>
```

The MVR commands are described below.

Command: Show MVR Configuration
Syntax: mvr config
Description: Show the current MVR configuration.

```
>mvr config
```

```
MVR Configuration:
```

```
=====
```

```
MVR Mode: Disabled
```

```
MVR Interface Setting
```

VID	Name	Mode	Tagging	Priority	LLQI
----	-----	-----	-----	-----	-----

```
MVR Immediate Leave Setting
```

Port	Immediate Leave
----	-----

1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled

```
>
```

Example 2:

```
>mvr config
```

```
MVR Configuration:
```

```
=====
```

```
MVR Mode: Enabled
```

```
MVR Interface Setting
```

VID	Name	Mode	Tagging	Priority	LLQI
----	-----	-----	-----	-----	-----

1	mvrvid01	Dynamic	Tagged	0	5
---	----------	---------	--------	---	---

```
[Port Setting of mvrvid01 (VID-1)]
```

```
Source Port : 2,4-7
```

```
Receiver Port: 3,8
```

```
Inactive Port: 1,9
```

```
[Channel Setting of mvrvid01 (VID-1)]
```

```
Name : mvrvidch01
```

```
Start Address: 239.0.0.0
```

```
End Address : 239.0.0.255
```

VID	Name	Mode	Tagging	Priority	LLQI
----	-----	-----	-----	-----	-----

2	mvrvid02	Compatible	Untagged	1	4
---	----------	------------	----------	---	---

```
[Port Setting of mvrvid02 (VID-2)]
```

```
Inactive Port: 1-9
```

```
[Channel Setting of mvrvid02 (VID-2)]
```

```
<Empty Channel Table>
```

```

MVR Immediate Leave Setting
Port  Immediate Leave
-----
1      Enabled
2      Enabled
3      Enabled
4      Disabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
>

```

Messages:

```

W mvr 03:10:02 57/mvr_stacking_set_intf_entry#1937: Warning: MVR delete VLAN-1 failed in isid-1
W mvr 03:10:02 57/mvr_stacking_set_intf_entry#1937: Warning: MVR delete VLAN-1 failed in isid-1

```

Command: Set / Show MVR Mode**Syntax:** **mvr mode** [enable|disable]

Description: Set or show system MVR mode, where:

- enable** : Enable MVR Mode.
- disable** : Disable MVR Mode.

(The default is 'Show MVR mode'.)

Example:

```

>mvr mode enable
>mvr mode disable
>mvr mode
MVR Mode: Disabled
>

```

Note that MVR mode and MVR Port mode must both be enabled for full S328x MVR functionality.

Command: **MVR VLAN Setup**
Syntax: **mvr vlan setup** [<mvid>] [add|del|upd] [(Name <mvr_name>)]
Description: Set or show per MVR VLAN configuration, where:
 <mvid> : MVR VLAN ID (1-4094)
add : Add operation
del : Delete operation
upd : Update operation
name : MVR Name keyword
 <mvr_name>: MVR VLAN name (maximum of 32 characters)

Example:

```
>mvr vlan setup 1 del
W mvr 20:55:15 10/mvr_stacking_set_intf_entry#1685: Warning: MVR delete VLAN-1 failed in isid-1
W mvr 20:55:15 10/mvr_stacking_set_intf_entry#1685: Warning: MVR delete VLAN-1 failed in isid-1
>mvr vlan setup 1 add
>mvr vlan setup 1 add
MVR VLAN already exists!
>mvr vlan setup 1
MVR Interface Setting
VID   Name
-----
1
[Port Setting of (VID-1)]
Inactive Port: 1-9
[Channel Setting of (VID-1)]
Name      : mvrvidch01
Start Address: 239.0.0.0
End Address  : 239.0.0.255
>
```

Messages:

Input MVR VID doesn't exist!

W mvr 20:55:15 10/mvr_stacking_set_intf_entry#1685: Warning: MVR delete VLAN-1 failed in isid-1

W mvr 22:01:59 46/_mvr_vlan_warning_handler#4112: Warning: Please adjust the management VLAN ports overlapped with MVR source ports!

Command: **MVR VLAN Mode**

Syntax: **mvr vlan mode** [<vid>|<mvr_name>] [dynamic|compatible]

Description: Set or show per MVR VLAN mode, where:
 <vid>|<mvr_name>: MVR VLAN ID (1-4094) or Name (maximum of 32 characters).
dynamic : Dynamic MVR mode.
compatible: Compatible MVR mode.
 (The default is 'Show MVR VLAN mode'.)

Example:

```
>mvr vlan mode 1 compatible
>mvr vlan setup 1
MVR Interface Setting
VID   Name
----  -----
1
[Port Setting of (VID-1)]
Inactive Port: 1-9
[Channel Setting of (VID-1)]
Name      : mvrvidch01
Start Address: 239.0.0.0
End Address : 239.0.0.255
```

VID	Name	Mode	Tagging	Priority	LLQI
1		Compatible	Tagged	0	5

Messages: *Input MVR VID doesn't exist!*
Invalid parameter: 1

Command: **MVR VLAN Port**

Syntax: **mvr vlan port** [<vid>|<mvr_name>] [<port_list>] [source|receiver|inactive]

Description: Set or show per MVR VLAN port role, where:
 <vid>|<mvr_name>: MVR VLAN ID (1-4094) or Name (up to 32 characters).
 <port_list> : Port list or 'All'. The default is 'All' ports.
source : MVR source port.
receiver : MVR receiver port.
inactive : Disable MVR.
 (The default is 'Show MVR port role'.)

Example:

```
>mvr vlan port 1
MVR Interface Setting
VID   Name
----  -----
1
[Port Setting of (VID-1)]
Inactive Port: 1-9
>mvr vlan port 1 1 source
>mvr vlan port 1
MVR Interface Setting
VID   Name
----  -----
1
[Port Setting of (VID-1)]
Source Port : 1
Inactive Port: 2-9
>
```

Messages: *Input MVR VID doesn't exist!*
Invalid parameter: one

Command: MVR VLAN LLQI

Syntax: **mvr vlan llqi** [<vid>|<mvr_name>] [mvr_param_llqi]

Description: Set or show per MVR VLAN LLQI (Last Listener Query Interval). The parameters are:
 <vid>|<mvr_name>: MVR VLAN ID (1-4094) or Name (up to 32 characters).
mvr_param_llqi : -1 : Default Value (5).

0~31744 : Last Listener Query Interval in tenths of seconds.

(The default is 'Show MVR Interface Last Listener Query Interval'.)

Example:

```
>mvr vlan llqi
MVR Interface Setting
VID      Name                               LLQI
-----  -
1        1                                           5
VID      Name                               LLQI
-----  -
2        mvrvid02                               4
>mvr vlan llqi 1 400
>mvr vlan llqi
MVR Interface Setting
VID      Name                               LLQI
-----  -
1        1                                           400
VID      Name                               LLQI
-----  -
2        mvrvid02                               4
>
```

Messages: *Input MVR VID doesn't exist!*
Invalid parameter: Name

Command: MVR VLAN Channel

Syntax: **mvr vlan channel** [<vid>|<mvr_name>] [add|del|upd] [channel] [channel_bound] [(Name <grp_name>)]

Description: Set or show per MVR VLAN channel, where:

<vid>|<mvr_name>: MVR VLAN ID (1-4094) or Name (up to 32 characters).

add : Add operation.

del : Delete operation.

upd : Update operation.

channel : IPv4/IPv6 multicast group address.

channel_bound : The boundary IPv4/IPv6 multicast group address for the channel.

The starting/ending IPv4/IPv6 Multicast Group Address that will be used as a streaming channel. For example:

<u>Start</u>	<u>End</u>	<u>Description</u>
224.0.0.0	224.0.0.255	Reserved for special “well-known” multicast addresses.
224.0.1.0	238.255.255.255	Globally-scoped (Internet-wide) multicast addresses.
239.0.0.0	239.255.255.255	Administratively-scoped (local) multicast addresses.

name : MVR Name keyword.

<grp_name> : MVR Channel name (up to 32 characters).

Example 1:

```
>mvr vlan channel
```

```
MVR Interface Setting
```

VID	Name	Mode	Tagging	Priority	LLQI
1	a1	Dynamic	Tagged	0	5

```
[Port Setting of a1(VID-1)]
```

```
Source Port : 2
```

```
Inactive Port: 1,3-8
```

```
[Channel Setting of a1(VID-1)]
```

```
Name : sbils
```

```
Start Address: 224.0.0.1
```

```
End Address : 224.0.0.10
```

Example 2:

```
>mvr vlan setup 1
```

```
MVR Interface Setting
```

VID	Name	Mode	Tagging	Priority	LLQI
1	mvrvid01	Dynamic	Tagged	0	5

```
[Port Setting of mvrvid01(VID-1)]
```

```
Inactive Port: 1-8
```

```
[Channel Setting of mvrvid01(VID-1)]
```

```
<Empty Channel Table>
```

```
>
```

Messages:

```
>W mvr 03:24:04 46/_mvr_vlan_warning_handler#4230: Warning: Please adjust the management VLAN ports overlapped with MVR source ports!
```

Command: MVR VLAN Priority

Syntax: **mvr vlan priority** [<vid>|<mvr_name>] [priority] [tagged|untagged]

Description: Set or show per MVR VLAN priority and VLAN tag, where:
 <vid>|<mvr_name>: MVR VLAN ID (1-4094) or Name (up to 32 characters).
priority : CoS priority value (0 - 7).
tagged : Tagged IGMP/MLD frames will be sent.
untagged : Untagged IGMP/MLD frames will be sent.

Example:

```
>mvr vlan priority
MVR Interface Setting
VID      Name                               Tagging  Priority
-----  -----
1                               Tagged   0
VID      Name                               Tagging  Priority
-----  -----
2      mvrvid02                             Untagged 1
>mvr vlan priority 2 3 tagged
>mvr vlan priority
MVR Interface Setting
VID      Name                               Tagging  Priority
-----  -----
1                               Tagged   0
VID      Name                               Tagging  Priority
-----  -----
2      mvrvid02                             Tagged   3
>
```

Messages: *Input MVR VID doesn't exist!*
Invalid parameter: 1

Command: MVR Immediate Leave

Syntax: **mvr immediate leave** [<port_list>] [enable|disable]

Description: Set or show MVR immediate leave per port, where:
<port_list>: Port list or 'All'. The default is 'All' ports.
enable : Enable Immediate Leave.
disable : Disable Immediate Leave.
(The default is 'Show MVR Immediate Leave'.)

```
Example: >mvr immediate leave
MVR Immediate Leave Setting
Port Immediate Leave
-----
1 Enabled
2 Enabled
3 Enabled
4 Disabled
5 Disabled
6 Disabled
7 Disabled
8 Disabled

>mvr immediate leave 1 disable
>mvr immediate leave
MVR Immediate Leave Setting
Port Immediate Leave
-----
1 Disabled
2 Enabled
3 Enabled
4 Disabled
5 Disabled
6 Disabled
7 Disabled
8 Disabled

>
```


Command: MVR Status

Syntax: **mvr status** [<vid>] [clear]

Description: Show or clear the current MVR operational status, where:
 <vid>: VLAN ID (1-4094).
clear : Clear log.

Example:

```
>mvr status
IPv4 Querier Rx Tx Rx Rx Rx Rx
VID Status Query Query V1 Join V2 Join V3 Join V2 Leave
-----
1 DISABLE 0 0 0 0 0 0

IPv6 Querier Rx Tx Rx Rx Rx
VID Status Query Query V1 Report V2 Report V1 Done
-----
1 DISABLE 0 0 0 0 0

IPv4 Querier Rx Tx Rx Rx Rx Rx
VID Status Query Query V1 Join V2 Join V3 Join V2 Leave
-----
2 DISABLE 0 0 0 0 0 0

IPv6 Querier Rx Tx Rx Rx Rx
VID Status Query Query V1 Report V2 Report V1 Done
-----
2 DISABLE 0 0 0 0 0

>
```

Command: MVR Groups

Syntax: **mvr groups** [<vid>]

Description: Show the MVR group addresses, where:
 <vid>: VLAN ID (1-4094).

Example: >mvr groups
 >

Command: MVR SFM

Syntax: **mvr sfm** [<vid>] [<port_list>]

Description: Show SFM (including SSM) related information for MVR, where:
 <vid> : VLAN ID (1-4094)
 <port_list>: Port list or 'All'. The default is 'All' ports.

Example: >mvr sfm
 >mvr sfm 1
 >mvr sfm all
 >

SFM is Source-Filtered Multicast and SSM is Source-Specific Multicast per IETF RFC 3569. For details see <http://www.ietf.org/rfc/rfc3569.txt>.

ERPS Commands

The ERP instance is an entity that is responsible for the protection of a subset of the VLANs that transport traffic over the physical Ethernet ring. Each ERP instance is independent of other ERP instances that may be configured on the physical Ethernet ring. The S3280 implements the ITU G.8032 standard for ERPS, which uses the APS automatic protection protocol for protection in ring and interconnected ring topology. The S3280 supports G.8032v1 in a single ring topology and G.8032v2 in multiple rings/ladder topologies.

ERPS specifies protection switching mechanisms and a protocol for Ethernet layer network (ETH) rings. Ethernet Rings can provide wide-area multipoint connectivity more economically due to their reduced number of links. The mechanisms and protocol defined in this Recommendation achieve highly reliable and stable protection; and never form loops, which would fatally affect network operation and service availability.

Each Ethernet Ring Node is connected to adjacent Ethernet Ring Nodes participating in the same Ethernet Ring, using two independent links. A ring link is bounded by two adjacent Ethernet Ring Nodes, and a port for a ring link is called a ring port. The minimum number of Ethernet Ring Nodes in an Ethernet Ring is two.

The ring protection switching architecture fundamentals are a) the principle of loop avoidance, and b) the use of learning, forwarding, and Filtering Database (FDB) mechanisms defined in the ETH_FF (Ethernet flow forwarding function).

Loop avoidance in an Ethernet Ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the Ring Protection Link (RPL), and under normal conditions this ring link is blocked (i.e., not used for service traffic). One designated Ethernet Ring Node, the 'RPL Owner Node', is responsible for blocking traffic at one end of the RPL. Under an Ethernet ring failure condition, the RPL Owner Node is responsible for unblocking its end of the RPL (unless the RPL has failed) allowing the RPL to be used for traffic. The other Ethernet Ring Node adjacent to the RPL, the 'RPL Neighbour Node', may also participate in blocking or unblocking its end of the RPL. The event of an Ethernet Ring failure results in protection switching of the traffic. This is achieved under the control of the ETH_FF functions on all Ethernet Ring Nodes. An APS protocol is used to coordinate the protection actions over the ring.

Note: The SOAM MEP configuration must be successfully completed before configuring Ethernet Ring Protection Switching (ERPS) using the commands in this section. See the "[MEP Commands](#)" on page 219.

These S3280 commands provide Ethernet Ring Protection Switching (ERPS) functions:

>**erps ?**

Available Commands:

```

Erps command [fs|ms|clear] <port> <group-id>
Erps version [v1|v2] <group-id>
Erps add <group-id> <east_port> <west_port> [major|sub] [interconnected] [virtual_channel] [<major-ring-id>]
Erps reversion [revertive|nonrevertive] <group-id>
Erps vlan add <vid> <group-id>
Erps vlan delete <vid> <group-id>
Erps mep <east_sf_mep> <west_sf_mep> <east_raps_mep> <west_raps_mep> <group-id>
Erps rpl neighbour <rpl_port> <group-id>
Erps rpl owner <rpl_port> <group-id>
Erps rpl neighbour clear <group-id>
Erps rpl owner clear <group-id>
Erps hold off timeout <hold_timeout> <group-id>
Erps guard-timeout <guard_timeout> <group-id>
Erps wtr-timeout <wtr_timeout> <group-id>
Erps delete <group-id>
Erps topologychange [propagate|nopropagate] <group-id>
Erps configuration [<group-id>] [statistics|clear]
>

```

The S3280 ERPS commands are explained below.

Command: **Configure / Clear ERPS Instance**

Syntax: **erps command** [fs|ms|clear] <port> <group-id>

Description: Used to configure an existing Ethernet Ring Protection Switch (ERPS) instance. Invokes an administrative command for a given protection group, where:

A port can be administratively configured to be in either Manual switch or Forced switch state or None (neither Forced or Manual).

FS (Forced Switch): forces a block on the ring port where the command is issued.

MS (Manual Switch): in the absence of a failure or FS, an MS selection forces a block on the ring port where the command is issued.

Clear: clears the active local administrative selection (e.g., Forced Switch or Manual Switch state). The Clear command is used for these operations:

- Clearing an active local administrative command (e.g., forced switch or manual switch),
- Triggering reversion before the WTR or WTB timer expires in case of revertive operation, and
- Triggering reversion in case of non-revertive operation.

<**port**> = a valid port number (1 - 9); forces a block on the ring port issuing this command.
 <**group-id**> = Protection Group ID number (1 - 64)

Example:

```

>erps command fs 1 1
incorrect error code = 4294967295
>erps command fs 1 1

given protection group does not exists
>erps command clear 1 1
>

```

Messages: *given protection group does not exists*
incorrect error code = 4294967295

Command: ERPS Configuration

Syntax: **erps config** [<group-id>] [statistics|clear]

Description: Display or delete a specified ERPS protection group, or display / clear a protection group's R-APS statistics. The parameters are:

<group-id> : the Protection Group ID.

[statistics] : for displaying R-APS statistics.

[clear] : for clearing R-APS statistics.

Example 1: for each ERPS ID:

```
>erps config 1
```

ERPS ID	Port_1	Port_0	Node Role	RPL Block	RPL Port
1	1	2	Non RPL	0	

Protected VLANs:

None

```
Protection Group State      :Active
Port 0 SF Mep               :2
Port 1 SF Mep               :1
Port 0 APS MEP              :2
Port 1 APS MEP              :1
WTR Timeout                 :1
WTB Timeout                  :5500
Hold-Off Timeout            :0
Guard Timeout                :500
Node Type                    :Major-Interconnected
Reversion                    :Revertive
Version                      :ERPS-V2 compatible
ERPSv2 Admin Command        :None
```

```
FSM State                    :PENDING
Port 0 Link Status           :Link Up
Port 1 Link Status           :Link Up
Port 0 Block Status          :UNBLOCKED
Port 1 Block Status          :BLOCKED
R-APS Transmission           :STOPPED
R-APS Port 0 Reception       :NONE
R-APS Port 1 Reception       :NONE
FOP Alarm                     :OFF
```

```
>erps config 1 statistics
```

```
RAPS PDU's Received:        0
RAPS PDU's dropped:         0
local SF Occured:           0
local SF cleared:           0
remote SF received:         0
remote FS received:         0
NR Messages sent:           0
```

```
>
```

Messages: *W erps 04:32:34 54/cli_parse_erps_statistics#998: Warning: ALL statistics|clear]*

*Example 2:***>erps config 2**

```

ERPS ID  Port_1  Port_0  Node Role  RPL Block  RPL Port
-----  -
2        2        1      Non RPL   0

```

Protected VLANS:
None

```

Protection Group State      :Active
Port 0 SF Mep               :1
Port 1 SF Mep               :2
Port 0 APS MEP              :1
Port 1 APS MEP              :2
WTR Timeout                 :1
WTB Timeout                 :5500
Hold-Off Timeout            :0
Guard Timeout               :500
Node Type                   :Sub-Interconnected
Major Ring ID               :1
Topology change propagation :Disabled
Virtual Channel              :With
Reversion                   :Revertive
Version                     :ERPS-V2 compatible
ERPSv2 Admin Command        :None

FSM State                   :PENDING
Port 0 Link Status          :Link Up
Port 1 Link Status          :Link Up
Port 0 Block Status         :BLOCKED
Port 1 Block Status         :BLOCKED
R-APS Transmission          :STOPPED
R-APS Port 0 Reception      :NONE
R-APS Port 1 Reception      :NONE
FOP Alarm                   :OFF

```

>

Command: Set ERPS Version**Syntax:** **erps version** [v1|v2] <group-id>**Description:** Specifies the protocol version for a given protection group, where:

[v1|v2] : specifies the protocol version for a given protection group (the ERPS protocol version to be supported).

v1 : G.8032 v1 supported a single ring topology. The v1 protocol is robust enough to work for unidirectional failure and multiple link failure scenarios in a ring topology. It allows mechanism to force switch (FS) or manual switch (MS) to take care of field maintenance scenario.**v2** : G.8032 v2 supports multiple rings/ladder topology. The v2 protocol also introduced other features such as Revertive/ Non-revertive mode after condition, that is causing the switch, is cleared, Administrative commands - Forced Switch (FS), Manual Switch (MS) for blocking a particular ring port, Flush FDB (Filtering database), and support of multiple ERP instances on a single ring.

<group_id> : protection group ID (1 - 64).

Example:
>**erps version v2 1**
>**Command: Add ERPS Group****Syntax:** **erps add** <group-id> <east-port> <west-port> [major|sub] [interconnected] [virtual_channel] [<major-ring-id>]**Description:** Create a new Ethernet ring protection group, where:

<group-id> : protection group id (1 - 64).

<east_port> : protection group east port (east port of a protection group).

<west_port> : protection group west port (west_port can be 0 for sub-rings).

[major|sub] : ring type (i.e., major-ring or sub-ring).

[interconnected] : interconnection node or not. Set for interconnected node.

[[virtual_channel] : Virtual channel present or not. Set for virtual channel.

[<major-ring-id>] : major ring group ID for interconnected sub-ring (major ring of a sub-ring, when configuring as an interconnected node).

Example:
>**erps add 1 1 1 interconnected virtual_channel 1**
east and west ports are same
>**erps add 1 1 2 interconnected virtual_channel 1**
>**erps add 1 2 3 interconnected virtual_channel 1**
>**Messages:***east and west ports are same**given protection group already crated***Command: Configure ERPS Reversion****Syntax:** **erps reversion** [revertive|nonrevertive] <group-id>**Description:** Use to configure reversion characteristics for a specified, existing node, where:

[revertive|nonrevertive] : enabling or disabling reversion for a given group.

<group_id> : protection group ID (1 - 64).

Example:
>**erps reversion revertive 1**
>**erps reversion revertive 2****Messages:** *given protection group does not exists*

Command: Add ERPS VLAN

Syntax: **erps vlan add** <vid> <group-id>

Description: Used to associate a specified VLAN to a protection group, where:
 <vid> : vlan to be protected; VLAN ID 1-4094.
 <group-id> : protection group-id to which VID belongs (1 - 64).

Example: >**erps vlan add 1 1**
>

Messages: *incorrect error code = 11 if the VLAN already exists.*

Command: Delete ERPS VLAN from a Group

Syntax: **erps vlan delete** <vid> <group-id>

Description: Use for disassociating a given VLAN to a protection group, where:
 <vid> : Protected VLAN to be deleted; VLAN ID 1-4094.
 <group-id> : Protection Group ID to which the VID belongs (1 - 64).

Example: >**erps vlan delete 2 2**

 vlans can not be deleted for this protection group
 >**erps vlan delete 1 1**
>

Messages: *vlans can not be deleted for this protection group*

Command: ERPS MEP (Associate an ERPS MEP with a Protection Group)

Syntax: **erps mep** <east_sf_mep> <west_sf_mep> <east_raps_mep> <west_raps_mep> <group-id>

Description: Used for associating Port 0/1 MEP to a Protection Group, where:
 <east_sf_mep> : MEP_ID for finding out Continuity Check errors on Port 0.
 <west_sf_mep> : MEP_ID for finding out Continuity Check errors on Port 1.
 <east_raps_mep> : MEP_ID for transmitting R-APS frames on Port 0.
 <west_raps_mep> : MEP_ID for transmitting R-APS frames on Port 1.
 <group_id> : Protection group ID for which MEP is associating (1 - 64).

The parameters are:

<east_sf_mep> : SF MEP ID for Port 0.
 <west_sf_mep> : SF MEP ID for Port 1.
 <east_raps_mep>: CC/RAPS MEP ID for Port 0.
 <west_raps_mep>: CC/RAPS MEP ID for Port 1.
 <group-id> : Protection Group ID (1 - 64).

Example: >**erps mep 1 1 2 1 2**

 given protection group does not exists
>

Messages:
given protection group does not exists
group association failed
incorrect error code = 36
Invalid <group-id> parameter: 0
mep association failed

Command: **Select ERPS RPL Neighbour**

Syntax: **erps rpl neighbour** <rpl_port> <group-id>

Description: Selection of RPL neighbour for a protection group, where:
 (east|west) : selects east or west as RPL neighbour.
 <group-id> : protection Group ID for selecting RPL Block.
 <rpl_port>: RPL Block.
 <group-id>: Protection Group ID (1 - 64).

Example:

```
>erps rpl neighbour 1 1
>erps rpl neighbour 2 0
>erps rpl neighbour 2 1
>
```

Messages:

```
given port is not configured either east or west for this group
given protection group does not exists
incorrect error code = 37
node is configured as neighbour for given group, can not set as rpl
```

Command: **Clear ERPS RPL Neighbour**

Syntax: **erps rpl neighbour clear** <group-id>

Description: Make this node a non-neighbour for a protection group, where:
 <group-id> : protection group ID for selecting RPL Block (protection group ID 1 - 64).

Example:

```
>erps rpl neighbour clear 1
>
```

Command: **Select ERPS RPL Owner**

Syntax: **erps rpl owner** <rpl_port> <group-id>

Description: Selection of RPL Block for a protection group; by default this node is considered an RPL Owner. The parameters are:
 (east|west) : selected east or west as RPL Block.
 <group-id> : protection group id for selecting RPL Block.
 <rpl_port>: RPL Block.
 <group-id>: protection group ID (1 - 64).

Example:

```
>erps rpl owner 1 1
>erps rpl owner 1 2
>erps rpl owner 1 2
>erps rpl owner 2 1
>
```

Messages:

```
failed in setting rpl block
given protection group does not exists
incorrect error code = 30
Invalid <group-id> parameter: 0
node is configured as neighbour for given group, can not set as rpl
this node is rpl owner for given protection group
```


Command: Clear ERPS RPL Owner**Syntax:** `erps rpl owner clear <group-id>`**Description:** Make a node a non-RPL Block for a protection group. On clearing, this node is no longer an RPL owner for the given group.**(east|west)** : Select east or west as RPL Block.**<group-id>** : Protection Group ID for selecting RPL Block (1-64).**Example:**

```
>erps rpl owner clear 1
>
```

Command: Set ERPS Holdoff Timeout**Syntax:** `erps holdoff-timeout <hold-timeout> <group-id>`**Description:** Used to configure the Hold-off timeout time for an existing Protection Group, where:**<hold_timeout>** :Hold-off timeout in milliseconds (0-10,000) in increments of 100 ms.**<group-id>** : Protection Group ID for configuring hold-off time (1 - 64).**Example:**

```
>erps holdoff-timeout 1 1
>erps holdoff-timeout 300 1
>erps holdoff-timeout 5000 2
>
```

Messages:
given protection group does not exists
hold off should be configured in multiples of 100 ms
*Invalid <hold_timeout> parameter: 1***Command: Set ERPS Guard Timeout****Syntax:** `erps guard-timeout <guard_timeout> <group-id>`**Description:** Used to configure the guard timeout time for an existing protection group, where:**<guard_timeout>**: the guard timeout in increments of 10 ms (milliseconds) in the range of 10 ms - 2000 ms (2 seconds).**<group-id>** protection group id for configuring guard time (1-64).**Example:**

```
>erps guard-timeout 100 1
>
```

Command: Set ERPS WTR Timeout**Syntax:** `erps wtr-timeout <wtr_timeout> <group-id>`**Description:** Used to configure wait-to-restore timeout for a protection group, in minutes, in the range of 1 to 12 minutes. The parameters are:**<wtr_timeout>** : the WTR timeout period. The valid range is 1 - 12 minutes.**<group-id>** : protection Group ID for configuring the WTR time.**Example:**

```
>erps wtr-timeout 8 1
>
```

Command: Delete ERPS Group**Syntax:** `erps delete <group-id>`**Description:** Used for deletion of an existing protection group, where:**<group-id>** : Protection Group ID (1 - 64) to be deleted.**Example:**

```
>erps delete 1
>
```

Command: Change ERPS Topology

Syntax: **erps topologychange** [propagate|nopropagate] <group-id>

Description: Used for specifying topology change propagation parameters for a given protection group. Topology change propagation, when enabled, sends a *Topology_Change* signal when a flush FDB action is triggered by the ERP Control Process of a Sub-Ring's ERP Instance. The *Topology_Change* signal is disabled after a period of 10 ms. The parameters are:
[propagate|nopropagate] : enable or disable topology change propagation for a specified Protection group.
<group_id> : the Protection Group ID (1 - 64) to be changed.

Example: >**erps topologychange propagate 1**
>

Messages: *given protection group does not exists*

LOAM Commands

OAM (Operation Administration and Maintenance) is a protocol described in ITU-T Y.1731 used to implement carrier ethernet functionality (e.g., CC and RDI). The Link OAM (LOAM) Link Event Configuration commands let you view and edit the current Link OAM Link Event configuration.

Enabling Link OAM provides network operators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions.

The Ethernet OAM protocol is used for monitoring and troubleshooting Ethernet networks. The S3280 supports the Link OAM standard IEEE 802.3–2005 Clause 57 which defines mechanisms for monitoring and troubleshooting Ethernet access links. Specifically it defines tools for discovery, remote failure indication, remote and local loopback, and status and performance monitoring. The S3280 supports Link OAM instance at every port. You can enable LOAM on any port(s). Consider the following when configuring LOAM on the S3280:

1. By default LOAM is disabled and set to Passive mode.
2. The LOAM unidirectional link feature is not supported.
3. The LOAM discovery process is interoperable with other vendor devices and should be able to perform LOAM loopback and event notifications with other vendor devices.
4. The LOAM loopback is supported on all ports and can perform line rate loopback of all the data plane traffic only.
5. The LOAM Dying gasp is supported; if all ports have LOAM operational, then the priority of sending a dying gasp will be over the uplink ports.
6. Link events include Errored Symbol Period, Errored Frame Event, and Errored Frame Period Event.
7. The LOAM counter statistics are available via all management interfaces, and an option to reset the LOAM counters is also available.
8. SNMP traps are generated for dying gasp events.

The S3280 commands provide Ethernet Link OAM (LOAM) functions:

>loam ?

Available Commands:

```

LOAM Control [<port_list>] [enable|disable]
LOAM Mode [<port_list>] [active|passive]
LOAM Mib-retrival-support [<port_list>] [enable|disable]
LOAM Variable-retrieve [<port_list>] [local-info|remote-info]
LOAM Remote_loopback_support [<port_list>] [enable|disable]
LOAM Remote_loopback_oper [<port_list>] [enable|disable]
LOAM Link_monitoring_support [<port_list>] [enable|disable]
LOAM Frame_error_event [<port_list>] [<error_window>] [<error_threshold>]
LOAM Symbol_period_error_event [<port_list>] [<error_window>] [<error_threshold>]
LOAM Frame_error_seconds_summary_event [<port_list>] [<error_window>] [<error_threshold>]
LOAM Status [<port_list>]
LOAM Link_monitor_status [<port_list>]
LOAM Statistics [<port_list>] [clear]
>

```

The S3280 LOAM commands are explained below.

Command: Set / Show LOAM Control

Syntax: loam control [<port_list>] [enable|disable]

Description: Set or show the existing Link OAM (LOAM) control capability, where:
 <port_list>: Port list or 'all'. The default is 'All' ports.
 enable : Enable Link OAM (LOAM).
 disable: Disable Link OAM (LOAM) (the default setting).

Example:

```
>loam control
Port  Port Mode
----  -
1     disabled
2     disabled
3     disabled
4     disabled
5     disabled
6     disabled
7     disabled
8     disabled
>loam control 4 disable
Requested configuration is already configured on port(1/4)
>loam control 1-4 enable
>loam control
Port  Port Mode
----  -
1     enabled
2     enabled
3     enabled
4     enabled
5     disabled
6     disabled
7     disabled
8     disabled
>
```

Messages: Requested configuration is already configured on port(1/4)

Command: Set / Show LOAM Mode

Syntax: **loam mode** [<port_list>] [active|passive]

Description: Set or show the existing Link OAM mode, where:

<port_list>: Port list or 'all'. The default is 'all' ports.

active : Enable Link OAM Active mode (disables LOAM Passive mode).

passive: Enable Link OAM Passive mode (disables LOAM Active mode) (the default setting).

Example:

```
>loam mode

Port  Port Mode
----  -
1     passive
2     passive
3     passive
4     passive
5     passive
6     passive
7     passive
8     passive
>loam mode 1-4 active
>loam mode

Port  Port Mode
----  -
1     active
2     active
3     active
4     active
5     passive
6     passive
7     passive
8     passive
>
```

Command: Set / Show LOAM MIB Retrieval Support

Syntax: `loam mib-retrieval-support [<port_list>] [enable|disable]`

Description: Set or show the MIB retrieval support, where:

<port_list>: Port list or 'all'. The default is 'All' ports.

enable : Enable MIB retrieval support; the DTE supports polling of various Link OAM-based MIB variables' contents.

disable: Disable MIB retrieval support. The default is all ports 'disabled'.

```

Example: >loam mib-retrieval-support
Port  MIB retrieval support
-----
1     disabled
2     disabled
3     disabled
4     disabled
5     disabled
6     disabled
7     disabled
8     disabled
>loam mib-retrieval-support 1-4 enable
>loam mib-retrieval-support
Port  MIB retrieval support
-----
1     enabled
2     enabled
3     enabled
4     enabled
5     disabled
6     disabled
7     disabled
8     disabled
>

```

Messages:

>E link_oam 22:53:06 61/eth_link_oam_mgmt_port_mib_retrieval_oper_set#849: Error: Unable to retrieve the mode of the port(1/43)

>E link_oam 23:02:10 61/eth_link_oam_mgmt_port_mib_retrieval_oper_set#910: Error: Error:7 occured while building MIB variable on port(1/0)

>loam mib-retrieval-support all enable

Requested configuration is already configured on port(1/1)

Recovery: Click the browser's back button to clear the message, verify your selection, and then try the operation again.

Command: **Set / Show LOAM variable-retrieve**
Syntax: **loam variable-retrieve** [<port_list>] [local-info|remote-info]
Description: Set or show MIB retrieval support, where:
 <port_list>: Port list or 'All'. The default is 'All' ports.
local-info : Enable MIB retrieval support.
remote-info: Disable MIB retrieval support.

Example:

```
>loam variable-retrieve
>loam variable-retrieve
Invalid request on this port
>loam variable-retrieve 1 local-info
>
```

Messages: *Invalid request on this port (ports 5-11)*
E link_oam 05:23:39 50/eth_link_oam_mgmt_port_mib_retrival_oper_set#910: Error:
Error:7 occured while building MIB variable on port(1/0)
Requested operation is already in progress

Command: **Set / Show LOAM Remote Loopback Support**
Syntax: **loam remote_loopback_support** [<port_list>] [enable|disable]
Description: Set or show remote loopback support, where:
 <port_list>: Port list or 'All'. The default is 'All' ports.
enable : Enable remote loopback support.
disable: Disable remote loopback support.

Example:

```
>loam remote_loopback_support

Port  Remote LoopBack support
----  -
1     disabled
2     disabled
3     disabled
4     disabled
5     disabled
6     disabled
7     disabled
8     disabled
>loam remote_loopback_support 1-4 enable
>loam remote_loopback_support

Port  Remote LoopBack support
----  -
1     enabled
2     enabled
3     enabled
4     enabled
5     disabled
6     disabled
7     disabled
8     disabled
>
```

Command: **Set / Show LOAM Remote Loopback Operation**

Syntax: **loam remote_loopback_oper** [<port_list>] [enable|disable]

Description: Set or show remote loopback operation, where:
 <port_list>: Port list or 'All'. The default is 'All' ports.
enable : Enable remote loopback operation.
disable: Disable remote loopback operation.

Example: >**loam remote_loopback_oper**
 Requested operation is already in progress
 >

Messages: *Link OAM is not enabled on the port(1/1)*
Requested configuration is not supported with the current OAM mode on port(1/1)
Requested operation is already in progress

Command: **Set / Show LOAM Link Monitoring Support**

Syntax: **loam link_monitoring_support** [<port_list>] [enable|disable]

Description: Set or show link monitoring support, where:
 <port_list>: Port list or 'All'. The default is 'All' ports.
enable : Enable link monitoring support (the default setting).
disable: Disable link monitoring support.

Example: >**loam link_monitoring_support**

```

Port  Link Monitoring support
-----
1     enabled
2     enabled
3     enabled
4     enabled
5     enabled
6     enabled
7     enabled
8     enabled
>loam link_monitoring_support 5-8 disable
>loam link_monitoring_support

Port  Link Monitoring support
-----
1     enabled
2     enabled
3     enabled
4     enabled
5     disabled
6     disabled
7     disabled
8     disabled
>
```


Command: Set / Show LOAM Frame Error Event

Syntax: `loam frame_error_event [<port_list>] [<error_window>] [<error_threshold>]`

Description: Set or show Frame Error Event parameters, where:

<port_list>: Port list or 'All'. The default is 'All' ports

error_window: Duration of the monitoring period in terms of seconds.
The Range is 1 - 60 seconds). The default is 1 second.

error_threshold: Number of permissible errors frames in the period defined by error_window. Range (0 - 0xffffffff) frames. The default is 0 frames.

Upbound value is not specified in the standard.

Example:

```
>loam frame_error_event
Port-No      Error_Window  Error_Threshold
-----
1             1             0
2             1             0
3             1             0
4             1             0
5             1             0
6             1             0
7             1             0
8             1             0
>loam frame_error_event 1 1 1
>loam frame_error_event 2 30 99
>loam frame_error_event 3 60 999
>loam frame_error_event
Port-No      Error_Window  Error_Threshold
-----
1             1             1
2             30            99
3             60            999
4             1             0
5             1             0
6             1             0
7             1             0
8             1             0
>
```

Command: Set / Show LOAM Symbol Period Error Event

Syntax: `loam symbol_period_error_event` [`<port_list>`][`<error_window>`][`<error_threshold>`][`<tx_threshold>`]

Description: Set or show parameters for Symbol Period Error Event, where:

<port_list>: Port list or 'All'. The default is 'All' ports.

error_window: Duration of the monitoring in terms of seconds. The range is 1 - 60 seconds. The default is 1 second.

error_threshold: Number of permissible error symbols in the period defined by 'error_window'. Range: 0 - 0xffffffff symbols. Default: 1 symbol.

CRC errors are treated as symbol errors. Upbound value is not specified in the standard.

Example:

```
>loam symbol_period_error_event
Port-No      Error_Window  Error_Threshold
-----
1             1             0
2             1             0
3             1             0
4             1             0
5             1             0
6             1             0
7             1             0
8             1             0
>loam symbol_period_error_event 1 1 1
>loam symbol_period_error_event 2 25 100
>loam symbol_period_error_event 3 45 250
>loam symbol_period_error_event
Port-No      Error_Window  Error_Threshold
-----
1             1             1
2             25            100
3             45            250
4             1             0
5             1             0
6             1             0
7             1             0
8             1             0
>
```

Command: Set / Show LOAM Frame Error Seconds Summary Event

Syntax: `loam frame_error_seconds_summary_event [<port_list>][<error_window>][<error_threshold>]`

Description: Set or show the parameters for Frame Error Seconds Summary Event, where:

<port_list>: Port list or 'all', default: All ports

error_window: Duration of the monitoring period in units of seconds.

The Range is 10 - 900 seconds. The Default is 10 seconds.

error_threshold: Number of permissible Error Frame Seconds in the period defined by 'error_window'.

The Range is 0 - 0xffff errored seconds. The Default is 1 errored second.

Upbound value is not specified in the standard.

Example:

```
>loam frame_error_seconds_summary_event
Port-No      Error_Window  Error_Threshold
-----
1             60           1
2             60           1
3             60           1
4             60           1
5             60           1
6             60           1
7             60           1
8             60           1
>loam frame_error_seconds_summary_event 1 15 2
>loam frame_error_seconds_summary_event 2 60 200
>loam frame_error_seconds_summary_event 3 400 999
>loam frame_error_seconds_summary_event
Port-No      Error_Window  Error_Threshold
-----
1             15           2
2             60           200
3             400          999
4             60           1
5             60           1
6             60           1
7             60           1
8             60           1
>
```

Messages: *Error In Configuration*

Command: Show Current LOAM Status

Syntax: loam status [<port_list>]

Description: Show the current Link OAM port status, where:
 <port_list>: Port list or 'All'. The default is 'All' ports.

Example 1:

```
>loam status 1

Port : 1
PDU permission: Info exchange
Discovery state: Active state
Remote MAC Address: -

Local client Remote Client
-----
port status: non operational -----
Mode: active -----
Unidirectional operation support: disabled -----
Remote loopback support: enabled -----
Link monitoring support: enabled -----
MIB retrieval support: disabled -----
MTU Size: 1500 -----
Multiplexer state: Forwarding -----
Parser state: Forwarding -----
OUI: 00-c0-f2 -----
PDU revision : 5 -----
>
```

Example 2:

```
>loam status 1

Port : 1
PDU permission: Receive only
Discovery state: Fault state
Remote MAC Address: -

Local client Remote Client
-----
port status: non operational -----
Mode: passive -----
Unidirectional operation support: disabled -----
Remote loopback support: disabled -----
Link monitoring support: enabled -----
MIB retrieval support: disabled -----
MTU Size: 1500 -----
Multiplexer state: Forwarding -----
Parser state: Forwarding -----
OUI: 00-c0-f2 -----
PDU revision : 0 -----
>
```

Command: Show Current LOAM Link Monitor Status

Syntax: loam link_monitor_status [<port_list>]

Description: Show the current Link OAM port link monitoring status, where:
<port_list>: Port list or 'All'. The default is 'All' ports.

Example: >loam link_monitor_status 1

```

Port : 1
Sequence number : 0
Symbol period error event Timestamp: 0
Symbol period error event window: 0
Symbol period error event threshold: 0
Symbol period errors: 0
Total symbol period errors: 0
Total symbol period error events: 0

Frame error event Timestamp: 0
Frame error event window: 0
Frame error event threshold: 0
Frame errors: 0
Total frame errors: 0
Total frame error events: 0

Frame period error event Timestamp: 0
Frame period error event window: 0
Frame period error event threshold: 0
Frame period errors: 0
Total frame period errors: 0
Total frame period error events: 0

Error Frame Seconds Summary Event Timestamp: 0
Error Frame Seconds Summary Event window: 0
Error Frame Seconds Summary Event Threshold: 0
Error Frame Seconds Summary Errors: 0
Total Error Frame Seconds Summary Errors: 0
Total Error Frame Seconds Summary Events: 0
>

```

Parameter Descriptions:

Port - The switch port number.

Event Name - the name of the Link Event which is being configured.

Window - represents the window period in the order of 100 msec. for the observation of various link events.

Period Threshold - represents the threshold value for the window period for the appropriate Link event so as to notify the peer of this error.

RxPacket Threshold - represents the threshold value for the window period for the errors in the received packets so as to notify the peer of this error.

Error Frame Event - counts the number of errored frames detected during the specified period. The period is specified by a time interval (Window in order of 100msec). This event is generated if the errored frame count is equal to or greater than the specified threshold for that period (Period Threshold). Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer.

Event Seconds Summary - the Errored Frame Seconds Summary Event TLV counts the number of errored frame seconds that occurred during the specified period. The period is specified by a time interval. This event is generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period. An errored frame second is a one second interval wherein at least one frame error was detected. Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer.

Symbol Period Error Event - the Errored Symbol Period Event counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period.

Frame Period Error Event - the Errored Frame Period Event TLV counts the number of errored frames detected during the specified period. The period is specified by a number of received frames. This event is generated if the errored frame count is greater than or equal to the specified threshold for that period (e.g., if the errored frame count is greater than or equal to 10 for the last 1,000,000 frames received). Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer.

Command: Show / Clear Current LOAM Statistics

Syntax: loam statistics [<port_list>] [clear]

Description: Show or clear the current Link OAM port statistics, where:
 <port_list>: Port list (1-8) or 'All'. The default is 'All ports'.
 clear : Clear log; resets counters to 0 and begins incrementing immediately.

```

Example: >loam statistics 1
1
PDU stats
-----
Information PDU TX:                2733
Information PDU RX:                0
Variable request PDU RX:          0
Variable request PDU TX:          0
Variable response PDU RX:         0
Variable response PDU TX:         0
Loopback PDU RX:                  0
Loopback PDU TX:                  0
Link Unique event notification PDU TX: 0
Link Unique event notification PDU RX: 0
Link Duplicate event notification PDU TX: 0
Link Duplicate event notification PDU RX: 0
Unsupported PDU RX:                0
Unsupported PDU TX:                0
Link Fault PDU TX:                 0
Link Fault PDU RX:                 0
Dying gasp PDU TX:                 0
Dying gasp PDU RX:                 0
Critical event PDU TX:             0
Critical event PDU RX:             0
>

```

Parameter Descriptions:

The displayed counters represent the total number of OAM frames received and transmitted for the selected port. Discontinuities of these counters can occur at re-initialization of the management system.

Receive Total and Transmit Total

Rx and Tx OAM Information PDU's: The number of received and transmitted OAM Information PDU's. Discontinuities of this counter can occur at re-initialization of the management system.

Rx and Tx Unique Error Event Notification: A count of the number of unique Event OAMPDUs received and transmitted on this interface. Event Notifications may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. Duplicate Event Notification transmissions are counted by Duplicate Event Notification counters for Tx and Rx respectively. A unique Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is distinct from the previously transmitted Event Notification OAMPDU Sequence Number.

Rx and Tx Duplicate Error Event Notification: A count of the number of duplicate Event OAMPDUs received and transmitted on this interface. Event Notification OAMPDUs may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. A duplicate Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is identical to the previously transmitted Event Notification OAMPDU Sequence Number.

Rx and Tx Loopback Control: A count of the number of Loopback Control OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Request: A count of the number of Variable Request OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Response: A count of the number of Variable Response OAMPDUs received and transmitted on this interface.

Rx and Tx Org Specific PDU's

A count of the number of Organization Specific OAMPDUs transmitted on this interface.

Rx and Tx Unsupported Codes: A count of the number of OAMPDUs transmitted on this interface with an unsupported op-code.

Rx and Tx Link fault PDU's: A count of the number of Link fault PDU's received and transmitted on this interface.

Rx and Tx Dying Gasp: A count of the number of Dying Gasp events received and transmitted on this interface (Last Gasp). The S3280 is equipped with the last gasp circuit for triggering a notification in the event of a power failure. This will be useful for sending a notification. The uplink ports have highest priority to send the notifications of last gasp. The last gasp can be in the form of IEEE802.3 2008 Clause 57 Dying gasp event and/or an SNMP trap to NMS system. The management interface provides an option to choose the preferred mode of notification (either a SNMP trap or an IEEE 802.3 2008 clause 57 event).

Rx and Tx Critical Event PDU's: A count of the number of Critical event PDU's received and transmitted on this interface.

Loop Protect Commands

The S3280 Loop Protect commands are used to define and display loop protection at the device and port level.

Loop protection increases the efficiency of STP, RSTP, and MSTP by preventing ports from going into a forwarding state that would result in a loop opening up in the network. In spanning tree topologies, a loop-free network is supported by the exchange of a BPDU. Peer STP applications running on the switch interfaces use BPDUs to communicate. The exchange of BPDUs ultimately determines which interfaces block traffic (preventing loops) and which interfaces become root ports and forward traffic. However, a blocking interface can transition to the forwarding state erroneously if the interface stops receiving BPDUs from its designated port on the segment. This transition error can occur with a hardware error on the switch or a software configuration error between the switch and its neighbor.

With loop protection enabled, the spanning tree topology detects root ports and blocked ports, and ensures that both keep receiving BPDUs. If a loop protection enabled interface quits receiving BPDUs from its designated port, it reacts as it would react to a problem with the physical connection on this interface. Rather than transition the interface to a forwarding state, it instead transitions it to a 'loop inconsistent' state. The interface recovers, and then it transitions back to the spanning tree blocking state when it receives a BPDU.

Loop protection is most effective when enabled in the entire switched network. You should generally enable loop protection on all switch interfaces that could become a root or designated port.

Note: If you will be using the S3280 Loop Protection function, enable Loop Protection here, both globally and at the port level, as one of the first overall configuration steps.

The available Loop Protect commands are listed below.

```
>loop ?
Available Commands:

Loop Protect Configuration
Loop Protect Mode [enable|disable]
Loop Protect Transmit [<transmit-time>]
Loop Protect Shutdown [<shutdown-time>]
Loop Protect Port Configuration [<port_list>]
Loop Protect Port Mode [<port_list>] [enable|disable]
Loop Protect Port Action [<port_list>] [shutdown|trap|log|shut_log|shut_trap|log_trap|all]
Loop Protect Port Transmit [<port_list>] [enable|disable]
Loop Protect Status [<port_list>]
>
```

Each of the available Loop Protect commands are explained below.

Command: Show Loop Protection Config
Syntax: loop protect configuration
Description: Displays the current Loop Protection settings.

```
Example: >loop protect config
Loop Protection Configuration:
=====
Loop Protection : Enabled
Transmission Time: 5
Shutdown Time : 180
>
```

Command: Set / Show Loop Protect Mode
Syntax: loop protect mode [enable|disable]
Description: Controls whether loop protection is enabled as a whole - globally (at the device level) or at the port level. Set or show the Loop Protection mode, where:
enable : Enable Loop Protection.
disable: Disable Loop Protection.

```
Example: >loop protect mode
Loop Protection : Enabled
>loop protect mode disable
>loop protect mode
Loop Protection : Disabled
>
```

Command: Set / Show Transmit Loop Protect
Syntax: loop protect transmit [<transmit-time>]
Description: Set or show the Loop Protection transmit interval. This is the interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds. The default is 5 seconds.

```
Example: >loop protect transmit
Transmission Time: 5
>loop protect transmit 7
>loop protect transmit
Transmission Time: 7
>
```

Command: Set / Show Loop Protect Shutdown Time

Syntax: loop protect shutdown [<shutdown-time>]

Description: Set or show the Loop Protection shutdown time. Shutdown time interval (0-604800 seconds). A value of zero disables re-enabling the port. This is the period (in seconds) for which a port will be kept disabled in the event a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until the next device restart). The default is 180 seconds (3 minutes).

Example:

```
>loop protect shutdown
Shutdown Time      : 180
>loop protect shutdown 2000
>loop protect shutdown
Shutdown Time      : 2000
>
```

Command: Show Loop Protect Port Config

Syntax: loop protect port configuration [<port_list>]

Description: Display the current Loop Protection port configuration, where:
 <port_list>: Port list or 'All'; the default is 'All' ports.

Example:

```
>loop protect port config
Port  Mode      Action          Transmit
----  -
1     Enabled    Log Only       Enabled
2     Enabled    Shutdown+Log   Enabled
3     Enabled    Shutdown+Log   Disabled
4     Enabled    Shutdown       Enabled
5     Enabled    Shutdown       Enabled
6     Enabled    Shutdown       Enabled
7     Enabled    Shutdown       Enabled
8     Enabled    Shutdown       Enabled
>loop protect port config 2
Port  Mode      Action          Transmit
----  -
2     Enabled    Shutdown+Log   Enabled
>
```

Command: Set / Show Loop Protect Port Mode

Syntax: loop protect port mode [<port_list>] [enable|disable]

Description: Set or show the Loop Protection port mode. This controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's. Parameters are:

<port_list>: Port list or 'All'. The default is 'All' ports.

enable : Enable Loop Protection mode (the default setting).

disable: Disable Loop Protection mode.

```
Example: >loop protect port mode
Port  Mode
-----
1     Enabled
2     Enabled
3     Enabled
4     Enabled
5     Enabled
6     Enabled
7     Enabled
8     Enabled
>loop protect port mode 4,5 disable
>loop protect port mode
Port  Mode
-----
1     Enabled
2     Enabled
3     Enabled
4     Disabled
5     Disabled
6     Enabled
7     Enabled
8     Enabled
>
```

Command: Loop Protect Port Action**Syntax:** **loop protect port action** [<port_list>] [shutdown|trap|log|shut_log|shut_trap|log_trap|all]**Description:** Set or show the Loop Protection port action. This command configures the action performed when a loop is detected on a port. For each port, the valid values are:

<port_list>: Port list or 'All'. The default is 'All' ports.

shutdown : Shutdown the port (only).**trap** : Send a trap only.**shut_trap** : Shutdown the port and send a trap.**log_trap** : Send a trap and Log the event.**all** : Shutdown the port, send a trap, and Log the event.**shut_log** : Shutdown the port and Log the event.**log** : Only Log the event.**Example:**

```

>loop protect port action

Port  Action
----  -
1     Shutdown
2     Shutdown
3     Shutdown
4     Shutdown
5     Shutdown
6     Shutdown
7     Shutdown
8     Shutdown

>loop protect port action 1,2 trap
>loop protect port action 3,4 shut_trap
>loop protect port action 5,6 shut_log
>loop protect port action 7,8 log
>loop protect port action

Port  Action
----  -
1     Trap Only
2     Trap Only
3     Shut+Trap
4     Shut+Trap
5     Shutdown+Log
6     Shutdown+Log
7     Log Only
8     Log Only
>

```

Messages:*Loop Detected: %s %ld %s", "Port", iport2uport(pstate->port), "shut down"**Loop Detected: %s %ld %s", "Port", iport2uport(pstate->port), ""**Loop Detected: %s %ld %s", "Port", iport2uport(pstate->port), "log"*

Command: **Loop Protect Port Transmit**

Syntax: **loop protect port transmit** [<port_list>] [enable|disable]

Description: Set or show the Loop Protection port transmit mode, where:

<port_list>: Port list or 'All'; the default is 'All' ports.

enable : Enable Loop Protection (the default setting).

disable: Disable Loop Protection.

```
Example: >loop protect port transmit
Port  Transmit
-----
1     Enabled
2     Enabled
3     Disabled
4     Enabled
5     Enabled
6     Enabled
7     Enabled
8     Enabled

>loop protect port transmit 7 disable
>loop protect port transmit
Port  Transmit
-----
1     Enabled
2     Enabled
3     Disabled
4     Enabled
5     Enabled
6     Enabled
7     Disabled
8     Enabled
>
```

Command: Show Loop Protect Status

Syntax: loop protect status [<port_list>]

Description: Display the current Loop Protection status information, where:
 <port_list>: Port list or 'All'. The default is 'All' ports.

Example:

```
>loop protect status
Port  Action          Transmit  Loops  Status  Loop  Time of Last Loop
-----
1     Shutdown+Log    Enabled   0      Up      -     -
2     Shutdown+Log    Enabled   0      Down   -     -
3     Shutdown+Log    Disabled  0      Down   -     -
4     Shutdown        Enabled   0      Down   -     -
5     Shutdown        Enabled   0      Down   -     -
6     Shutdown        Enabled   0      Down   -     -
7     Shutdown        Enabled   0      Down   -     -
8     Shutdown        Enabled   0      Down   -     -
>
```

IPMC Commands

These S3280 IPMC (IP Multimedia Communications) commands provide Multicast Listener Discovery (MLD) and Internet Group Management Protocol (IGMP) snooping functions.

IPMC (IP Multimedia Communications) refers to communication protocols and systems that operate over an IP network, including the Internet, enabling voice (VoIP), instant messaging (IM), whiteboarding, application sharing, and other forms of multimedia communication.

IGMP (Internet Group Management Protocol) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

MLD (Multicast Listener Discovery) is a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 similar to IGMPv3. The MLD protocol is described in RFC 3810 which has been updated by RFC 4604. Windows Vista and later support MLDv2. The Linux kernel has supported MLDv2 since v 2.5.68.

The S3280 IPMC commands include:

>**ipmc ?**

Available Commands:

IPMC Configuration [mld|igmp]
IPMC Mode [mld|igmp] [enable|disable]
IPMC Flooding [mld|igmp] [enable|disable]
IPMC Leave Proxy [mld|igmp] [enable|disable]
IPMC Proxy [mld|igmp] [enable|disable]
IPMC SSM [mld|igmp] [(Range <prefix> <mask_len>)]
IPMC VLAN Add [mld|igmp] <vid>
IPMC VLAN Delete [mld|igmp] <vid>
IPMC State [mld|igmp] [<vid>] [enable|disable]
IPMC Querier [mld|igmp] [<vid>] [enable|disable]
IPMC Compatibility [mld|igmp] [<vid>] [auto|v1|v2|v3]
IPMC Fastleave [mld|igmp] [<port_list>] [enable|disable]
IPMC Throttling [mld|igmp] [<port_list>] [limit_group_number]
IPMC Filtering [mld|igmp] [<port_list>] [add|del] [group_addr]
IPMC Router [mld|igmp] [<port_list>] [enable|disable]
IPMC Status [mld|igmp] [<vid>]
IPMC Groups [mld|igmp] [<vid>]
IPMC Version [mld|igmp] [<vid>]
IPMC SFM [mld|igmp] [<vid>] [<port_list>]
IPMC Parameter RV [mld|igmp] [<vid>] [ipmc_param_rv]
IPMC Parameter QI [mld|igmp] [<vid>] [ipmc_param_qi]
IPMC Parameter QRI [mld|igmp] [<vid>] [ipmc_param_qri]
IPMC Parameter LLQI [mld|igmp] [<vid>] [ipmc_param_llqi]
IPMC Parameter URI [mld|igmp] [<vid>] [ipmc_param_uri]

The S3280 IPMC commands are explained below.

Command: Show Current IPMC Configuration

Syntax: ipmc configuration [mld|igmp]

Description: Display the current IPMC snooping configuration, where:
mld : IPMC for IPv6 MLD.
igmp: IPMC for IPv4 IGMP.

Example 1: IPMC Configuration - IGMP:

```
>ipmc configuration igmp
```

```
IGMP Configuration:
```

```
=====
```

```
IGMP Mode: Disabled
IGMP SSM Range: 232.0.0.0/8
IGMP Leave Proxy: Disabled
IGMP Proxy: Disabled
IGMP Flooding Control: Enabled
```

```
IGMP Interface Setting
```

VID	State	Querier	Compatibility	RV	QI	QRI	LLQI	URI
1	Disabled	Enabled	IGMP-Auto	2	125	100	10	1

```
IGMP Port Status ( Router-Port Fast-Leave Throttling )
```

Port	Router	Dynamic Router	Fast Leave	Group Throttling Number
1	Disabled	No	Disabled	Unlimited
2	Disabled	No	Disabled	Unlimited
3	Disabled	No	Disabled	Unlimited
4	Disabled	No	Disabled	Unlimited
5	Disabled	No	Disabled	Unlimited
6	Disabled	No	Disabled	Unlimited
7	Disabled	No	Disabled	Unlimited
8	Disabled	No	Disabled	Unlimited

```
IGMP Group Filtering Setting
```

Port	Filtering Groups
1	No Filtering Group
2	No Filtering Group
3	No Filtering Group
4	No Filtering Group
5	No Filtering Group
6	No Filtering Group
7	No Filtering Group
8	No Filtering Group

Messages: (Please create IGMP Interfaces) if none exist.

Example 2: IPMC Configuration - MLD:

```
>ipmc configuration mld
```

```
MLD Configuration:
```

```
=====
```

```
MLD Mode: Disabled
MLD SSM Range: ff3e::/96
MLD Leave Proxy: Disabled
MLD Proxy: Disabled
MLD Flooding Control: Enabled
```

```
MLD Interface Setting
```

VID	State	Querier	Compatibility	RV	QI	QRI	LLQI	URI
1	Disabled	Enabled	MLD-Auto	2	125	100	10	1

```
MLD Port Status ( Router-Port Fast-Leave Throttling )
```

Port	Router	Dynamic Router	Fast Leave	Group Throttling Number
1	Disabled	No	Disabled	Unlimited
2	Disabled	No	Disabled	Unlimited
3	Disabled	No	Disabled	Unlimited
4	Disabled	No	Disabled	Unlimited
5	Disabled	No	Disabled	Unlimited
6	Disabled	No	Disabled	Unlimited
7	Disabled	No	Disabled	Unlimited
8	Disabled	No	Disabled	Unlimited

```
MLD Group Filtering Setting
```

Port	Filtering Groups
1	No Filtering Group
2	No Filtering Group
3	No Filtering Group
4	No Filtering Group
5	No Filtering Group
6	No Filtering Group
7	No Filtering Group
8	No Filtering Group

```
>
```

Command: **Set / Show IPMC Mode**
Syntax: **ipmc mode [mld|igmp] [enable|disable]**
Description: Set or show the IPMC snooping mode, where:
mld : IPMC for IPv6 MLD.
igmp: IPMC for IPv4 IGMP.
enable : Enable IPMC snooping.
disable: Disable IPMC snooping.
(The default is 'Show global IPMC snooping mode'.)

Example:

```
>ipmc mode mld enable
>ipmc mode mld
MLD Mode: Enabled
>ipmc mode mld enable
>ipmc mode igmp enable
>ipmc mode
IGMP Mode: Enabled
MLD Mode: Enabled
```

Command: **Set / Show IPMC Flooding**
Syntax: **ipmc flooding [mld|igmp] [enable|disable]**
Description: Set or show the IPMC unregistered addresses flooding operation, where:
mld : IPMC for IPv6 MLD.
igmp: IPMC for IPv4 IGMP.
enable : Enable IPMC flooding.
disable: Disable IPMC flooding.
(The default is 'Show IPMC flooding mode'.)

Example:

```
>ipmc flooding
IGMP Flooding Control: Enabled

MLD Flooding Control: Enabled
>ipmc flooding mld disable
>ipmc flooding mld
MLD Flooding Control: Disabled
>
```

Command: **Set / Show IPMC Leave Proxy**
Syntax: **ipmc leave proxy [mld|igmp] [enable|disable]**
Description: Set or show the mode of IPMC Leave Proxy, where:
mld : IPMC for IPv6 MLD.
igmp: IPMC for IPv4 IGMP.
enable : Enable IPMC Leave Proxy.
disable: Disable IPMC Leave Proxy.
(The default is 'Show IPMC Leave Proxy mode'.)

Example:

```
>ipmc leave proxy
IGMP Leave Proxy: Disabled

MLD Leave Proxy: Disabled
>ipmc leave proxy igmp enable
>ipmc leave proxy
IGMP Leave Proxy: Enabled

MLD Leave Proxy: Disabled
>
```

Command: **Set / Show IPMC Proxy**
Syntax: **ipmc proxy [mld|igmp] [enable|disable]**
Description: Set or show the mode of IPMC Proxy, where:
mld : IPMC for IPv6 MLD.
igmp: IPMC for IPv4 IGMP.
enable : Enable IPMC Proxy.
disable: Disable IPMC Proxy.
(The default is 'Show IPMC Proxy mode'.)

Example:

```
>ipmc proxy
IGMP Proxy: Disabled

MLD Proxy: Disabled
>
```

Command: **Set / Show IPMC SSM**
Syntax: **ipmc ssm [mld|igmp] [(Range <prefix> <mask_len>)]**
Description: Set or show the IPMC SSM Range, where:
mld : IPMC for IPv6 MLD.
igmp: IPMC for IPv4 IGMP.
range : SSM Range keyword.
<prefix> : IPv4/IPv6 multicast group address, accordingly.
<mask_len>: Mask length for IPv4(4 ~ 32)/IPv6(8 ~ 128) ssm range, accordingly

Example:

```
>ipmc ssm
IGMP SSM Range: 232.0.0.0/8

MLD SSM Range: ff3e::/96
>
```

Command: **Add IPMC VLAN**
Syntax: **ipmc vlan add [mld|igmp] <vid>**
Description: Add a new IPMC snooping VLAN interface, where:
mld|igmp: **mld** : IPMC for IPv6 MLD.
igmp: IPMC for IPv4 IGMP.
<vid> : VLAN ID (1-4094).

Example:

```
>ipmc vlan add mld 1
>
```

Messages: *MLD VLAN Interface already exists!*

Command: **Delete IPMC VLAN**
Syntax: **ipmc vlan delete [mld|igmp] <vid>**
Description: Delete an existing IPMC snooping VLAN interface, where:
mld|igmp: **mld** : IPMC for IPv6 MLD.
igmp: IPMC for IPv4 IGMP.
<vid> : VLAN ID (1-4094).

Example:

```
>ipmc vlan delete mld 1
>
```

Messages: *MLD VLAN Interface doesn't exist!*

Command: Set / Show IPMC State

Syntax: ipmc state [mld|igmp] [<vid>] [enable|disable]

Description: Set or show the IPMC snooping state for VLAN, where:

mld : IPMC for IPv6 MLD.

igmp: IPMC for IPv4 IGMP.

<vid> : VLAN ID (1-4094) or 'Any'. The default is 'Show all VLANs'.

enable : Enable MLD snooping.

disable: Disable MLD snooping.

Example:

```
>ipmc state
IGMP Interface Setting
VID   State
----  -
1     Disabled

MLD Interface Setting
VID   State
----  -
1     Disabled
>
```

Messages: Non-Existing MLD Interface ID 1000

Command: Set / Show IPMC Querier

Syntax: ipmc querier [mld|igmp] [<vid>] [enable|disable]

Description: Set or show the IPMC snooping querier mode for VLAN, where:

mld : IPMC for IPv6 MLD.

igmp: IPMC for IPv4 IGMP.

<vid> : VLAN ID (1-4094) or 'Any'. The default is 'Show all VLANs'.

enable : Enable IPMC querier.

disable : Disable IPMC querier.

Example:

```
>ipmc querier
IGMP Interface Setting
VID   Querier
----  -
1     Enabled

MLD Interface Setting
VID   Querier
----  -
1     Enabled
>
```

Command: Set / Show IPMC Compatibility

Syntax: ipmc compatibility [mld|igmp] [<vid>] [auto|v1|v2|v3]

Description: Set or show the IPMC compatibility, where:

mld : IPMC for IPv6 MLD.

igmp: IPMC for IPv4 IGMP.

<vid> : VLAN ID (1-4094) or 'Any'. The default is 'Show all VLANs'.

auto : Auto Compatibility (the default value).

v1 : Forced Compatibility of IGMPv1 or MLDv1.

v2 : Forced Compatibility of IGMPv2 or MLDv2.

v3 : Forced Compatibility of IGMPv3.

(The default is 'Show IPMC Interface Compatibility'.)

Example:

```
>ipmc compatibility
IGMP Interface Setting
VID      Compatibility
-----  -
1
MLD Interface Setting
VID      Compatibility
-----  -
1
>
```

Command: Set / Show IPMC Fastleave

Syntax: `ipmc fastleave [mld|igmp] [<port_list>] [enable|disable]`

Description: Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is 'pruned' from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

Set or show the IPMC snooping fast leave port mode, where:

mld : IPMC for IPv6 MLD.

igmp: IPMC for IPv4 IGMP.

<port_list>: Port list or 'All'. The default is 'All ports'.

enable : Enable IPMC fast leave.

disable : Disable IPMC fast leave.

(The default is 'Show IPMC fast leave mode'.)

Example: `>ipmc fastleave 1`

```
IGMP Port Status ( Fast-Leave )

Port  Fast Leave
----  -
1     Disabled

MLD Port Status ( Fast-Leave )

Port  Fast Leave
----  -
1     Disabled

>
```

Command: Set / Show IPMC Throttling

Syntax: ipmc throttling [mld|igmp] [<port_list>] [limit_group_number]

Description: Throttling can be enabled to limit the number of multicast groups to which a switch port can belong. Set or show the IPMC port throttling status, where:

mld : IPMC for IPv6 MLD.

igmp: IPMC for IPv4 IGMP.

<port_list>: Port list or 'All'. The default is 'All' ports.

0 : No limit.

1~10 : Group learn limit.

(The default is 'Show IPMC Port Throttling'.)

Example: >ipmc throttling 1

```
IGMP Port Status ( Throttling )
```

```
Port  Group Throttling Number
```

```
-----
```

```
1      Unlimited
```

```
MLD Port Status ( Throttling )
```

```
Port  Group Throttling Number
```

```
-----
```

```
1      Unlimited
```

```
>
```

Command: Set / Show IPMC Filtering

Syntax: ipmc filtering [mld|igmp] [<port_list>] [add|del] [group_addr]

Description: Set or show the IPMC port group filtering list, where:

mld : IPMC for IPv6 MLD.

igmp: IPMC for IPv4 IGMP.

<port_list>: Port list or 'all'. The default is 'All' ports.

add : Add new port group filtering entry.

del : Del existing port group filtering entry.

(The default is 'Show IPMC port group filtering list'.)

group_addr : IPv4/IPv6 multicast group address, accordingly

Example: >ipmc filtering 1

```
IGMP Group Filtering Setting
```

```
Port  Filtering Groups
```

```
-----
```

```
1      No Filtering Group
```

```
MLD Group Filtering Setting
```

```
Port  Filtering Groups
```

```
-----
```

```
1      No Filtering Group
```

```
>
```


Command: **Set / Show IPMC Router Port Mode**
Syntax: **ipmc router [mld|igmp] [<port_list>] [enable|disable]**
Description: Set or show the IPMC snooping router port mode, where:
mld : IPMC for IPv6 MLD.
igmp: IPMC for IPv4 IGMP.
<port_list>: Port list or 'All'. The default is 'All' ports.
enable : Enable IPMC router port.
disable : Disable IPMC router port.
(The default is 'Show IPMC router port mode'.)

Example:

```
>ipmc router 1 enable mld
Invalid parameter: mld

Syntax:
IPMC Router [mld|igmp] [<port_list>] [enable|disable]
>ipmc router mld 1 enable
>ipmc router 1

IGMP Port Status ( Router-Port )

Port  Router      Dynamic Router
----  -
1     Disabled    No

MLD Port Status ( Router-Port )

Port  Router      Dynamic Router
----  -
1     Enabled     No
>
```

Command: **Show Current IPMC Status**
Syntax: **ipmc status [mld|igmp] [<vid>]**
Description: Display the current IPMC operational status, where:
mld : IPMC for IPv6 MLD.
igmp: IPMC for IPv4 IGMP.
<vid> : VLAN ID (1-4094) or 'Any'. The default is 'Show all VLANs'.

Example:

```
>ipmc status mld any

  Querier  Rx      Tx      Rx      Rx      Rx
VID  Status  Query  Query  V1 Report  V2 Report  V1 Done
----  -
1    ACTIVE  0      4      0      0      0
>
```

Messages: *Please specify IPMC version: [mld|igmp]*

Command: Show IPMC Groups

Syntax: ipmc groups [mld|igmp] [<vid>]

Description: Show IPMC group addresses, where:

mld : IPMC for IPv6 MLD.

igmp: IPMC for IPv4 IGMP.

<vid> : VLAN ID (1-4094) or 'Any'. The default is 'Show all' VLANs.

Example:

```
>ipmc groups
Please specify IPMC version: [mld|igmp]
>ipmc groups mld
>ipmc groups
Please specify IPMC version: [mld|igmp]
>ipmc groups igmp 1
>ipmc groups igmp 1 ?
Description:
-----
Show IPMC group addresses, accordingly.

Syntax:
-----
IPMC Groups [mld|igmp] [<vid>]

Parameters:
-----
mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP

<vid>    : VLAN ID (1-4094) or 'any', default: Show all VLANs
>ipmc groups mld 1
>
```

Command: Show IPMC Version

Syntax: ipmc version [mld|igmp] [<vid>]

Description: Show the current IPMC versions, where:

mld : IPMC for IPv6 MLD.

igmp: IPMC for IPv4 IGMP.

<vid> : VLAN ID (1-4094) or 'Any'. The default is 'Show all' VLANs.

Example:

```
>ipmc version
Please specify IPMC version: [mld|igmp]
>ipmc version 1
Please specify IPMC version: [mld|igmp]
>ipmc version mld
>ipmc version igmp 1
>
```

Command: Show IPMC SFM

Syntax: ipmc sfm [mld|igmp] [<vid>] [<port_list>]

Description: Show SFM (including SSM) related information for IPMC, where:

mld : IPMC for IPv6 MLD.

igmp: IPMC for IPv4 IGMP.

<vid> : VLAN ID (1-4094) or 'Any'. The default is 'Show all VLANs'.

<port_list>: Port list or 'All'. The default is 'All' ports.

Example:

```
>ipmc sfm
Please specify IPMC version: [mld|igmp]
>ipmc sfm mld 1 1
>
```

SFM is Source-Filtered Multicast and SSM is Source-Specific Multicast per IETF RFC 3569. For details see <http://www.ietf.org/rfc/rfc3569.txt>.

Command: Set / Show IPMC Parameter RV

Syntax: ipmc parameter rv [mld|igmp] [<vid>] [ipmc_param_rv]

Description: Set or show the IPMC Robustness Variable, where:

mld : IPMC for IPv6 MLD.

igmp: IPMC for IPv4 IGMP.

<vid> : VLAN ID (1-4094) or 'any'. The default is 'Show all VLANs'.

ipmc_param_rv:

-1 : Default Value (2).

1~255 : Robustness Variable (RV).

(The default is 'Show IPMC Interface Robustness Variable'.)

Example:

```
>ipmc parameter rv

IGMP Interface Setting

VID    RV
----  ---
1      2
10     2
20     2
100    2
200    2

MLD Interface Setting

VID    RV
----  ---
1      2
10     2
20
100
200
>
```

Command: Set / Show IPMC Parameter QI

Syntax: ipmc parameter qi [mld|igmp] [<vid>] [ipmc_param_qi]

Description: Set or show the IPMC Query Interval. The Query Interval (QI) is the interval between General Queries sent by the Querier. The valid range is 1 to 255 seconds. The default is 125 seconds.

The parameters are:

mld : IPMC for IPv6 MLD.

igmp: IPMC for IPv4 IGMP.

<vid> : VLAN ID (1-4094) or 'Any'. The default is 'Show all VLANs'.

ipmc_param_qi:

-1 : Default Value (125).

1~31744 : Query Interval in seconds.

(The default is 'Show IPMC Interface Query Interval'.).

Example: >ipmc parameter qi

```
IGMP Interface Setting
```

```
VID    QI
```

```
-----
```

```
1
```

```
MLD Interface Setting
```

```
VID    QI
```

```
-----
```

```
1      125
```

```
>
```

Command: Set / Show IPMC Parameter QRI

Syntax: ipmc parameter qri [mld|igmp] [<vid>] [ipmc_param_qri]

Description: Set or show the IPMC Query Response Interval.

The QRI is the maximum response time used to calculate the Max Resp Code inserted into the periodic General Queries. The valid range is 0 to 31744 in tenths of a second. The default query response interval is 100 in tenths of a second (10 seconds). The parameters are:

mld : IPMC for IPv6 MLD.

igmp: IPMC for IPv4 IGMP.

<vid> : VLAN ID (1-4094) or 'any'. The default is 'Show all VLANs'.

ipmc_param_qri:

-1 : Default Value (100).

0~31744 : Query Response Interval in tenths of seconds.

(The default is 'Show IPMC Interface Query Response Interval')

Example:

```
>ipmc parameter qri

IGMP Interface Setting

VID    QRI
----  -
1

MLD Interface Setting

VID    QRI
----  -
1      100
>
>
```

Command: Set / Show IPMC Parameter LLQI

Syntax: ipmc parameter llqi [mld|igmp] [<vid>] [ipmc_param_llqi]

Description: Set or show the IPMC Last Listener Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The valid range is 0 to 31744 in tenths of a second. The default last member query interval is 10 in tenths of a second (1 second). The parameters are:

mld : IPMC for IPv6 MLD.

igmp : IPMC for IPv4 IGMP.

<vid> : VLAN ID (1-4094) or 'Any'. The default is 'Show all VLANs'.

ipmc_param_llqi:

-1 : Default Value (10).

0~31744 : Last Listener Query Interval in tenths of seconds.

(The default is 'Show IPMC Interface Last Listener Query Interval').

Example: >ipmc parameter llqi

```
IGMP Interface Setting
```

```
VID    LLQI
----  -
1
```

```
MLD Interface Setting
```

```
VID    LLQI
----  -
1      10
>
```

Command: Set / Show IPMC Parameter URI

Syntax: ipmc parameter uri [mld|igmp] [<vid>] [ipmc_param_uri]

Description: Set or show the IPMC Unsolicited Report Interval. The Unsolicited Report Interval (URI) is the time between repetitions of a host's initial report of membership in a group.

The valid range is 0 to 31744 seconds. The default unsolicited report interval is 1 second.

The parameters are:

mld : IPMC for IPv6 MLD.

igmp: IPMC for IPv4 IGMP.

<vid> : VLAN ID (1-4094) or 'Any'. The default is 'Show all VLANs'.

ipmc_param_uri:

-1 : Default Value (1).

0~31744 : Unsolicited Report Interval in seconds.

(The default is 'Show IPMC Interface Unsolicited Report Interval'.)

Example:

```
>ipmc parameter uri
IGMP Interface Setting
VID    URI
----  -
1
MLD Interface Setting
VID    URI
----  -
1      1
>
```

sFlow Commands

The S3280 sFlow Receiver configuration and sFlow Sampler can be monitored and modified via CLI commands. One Receiver is supported. The commands are for configuring sFlow Receiver IP type, sFlow Receiver IP Address, and Port Number for each sFlow Receiver.

The sFlow (sample Flow) protocol is used to monitor the sampled traffic on the S3280. The sFlow Agent configures the sampling rate at which the samples will be collected. The sFlow collector is configured to send the sample data to an external traffic monitoring application.

The sFlow 'Agent' uses sampling technology to capture traffic statistics from the device it is monitoring. The sFlow 'Datagrams' are used to immediately forward the sampled traffic statistics to an sFlow Collector for analysis. See http://www.sflow.org/sflow_version_5.txt for more information. The counter poller uses generic interface counters per IETF RFC 2233. See <http://tools.ietf.org/html/rfc2233#page-17> for more information.

The sFlow configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers. sFlow configuration is not persisted to non-volatile memory, which means that a reboot or master change will disable sFlow sampling.

Basically, sFlow can be configured in two ways: 1) via local management using the Web or CLI interface or 2) via SNMP. The owner of the current sFlow configuration assumes values as follows:

- If sFlow is currently unconfigured/unclaimed, **Owner** is *<none>*.
- If sFlow is currently configured via Web or CLI, **Owner** is *<Configured through local management>*.
- If sFlow is currently configured through SNMP, **Owner** contains a string identifying the sFlow receiver. If sFlow is configured through SNMP, all controls (except for the web interface Release button) are disabled to avoid inadvertent reconfiguration.

The S3280 sFlow commands include:

>**sflow ?**

Available Commands:

sFlow Configuration

sFlow Receiver [release] [<timeout>] [<ip_addr_host>] [<udp_port>] [<datagram_size>]

sFlow FlowSampler [<port_list>] [<sampling_rate>] [<max_hdr_size>]

sFlow CounterPoller [<port_list>] [<interval>]

sFlow Statistics Receiver [clear]

sFlow Statistics Samplers [<port_list>] [clear]

>

The S3280 sFlow commands are described below.

Command: Show sFlow Configuration
Syntax: sflow config
Description: Show global and per port sFlow configuration.
Example: >sflow config

```
sFlow Configuration:
=====

Receiver Configuration:
=====

Owner          : <none>
Receiver       : 0.0.0.0
UDP Port       : 6343
Max. Datagram : 1400 bytes
Time left      : 0 seconds

No enabled receivers. Skipping displaying per-port info.
>
```

Command: Set / Show sFlow Receiver
Syntax: sflow receiver [release] [<timeout>] [<ip_addr_host>] [<udp_port>] [<datagram_size>]
Description: Set or show the sFlow receiver timeout, IP address, and UDP port, where:

release : Release the current owner of the receiver.
 The owner can either be "<none>" if the receiver is not currently owned by anyone, it can be "<Configured through local management>" if it's currently set up by CLI or Web, or it can be anything else if is set-up via SNMP.
 You can only (re-)configure the receiver if it is not currently owned by anyone or owned by CLI or Web interface.
 If this argument is specified, the remaining arguments are ignored.

<timeout> : Receiver timeout measured in seconds. The switch decrements the timeout once per second, and as long as it is non-zero, the receiver receives samples.
 Once the timeout reaches 0, the receiver and all its configuration is reset to the default settings. The valid range is 0 - 2147483647 seconds.

<ip_addr_host> : IPv4/IPv6 address or a hostname identifying the receiver.

<udp_port> : Receiver's UDP port. The valid range is 0 - 65535.
 Use 0 to get the default port (which is 6343).

<datagram_size>: Maximum datagram size. The valid range is 200 - 1468 bytes.
 The default is 1400 bytes.

Example: >sflow receiver

```
Receiver Configuration:
=====

Owner          : <none>
Receiver       : 0.0.0.0
UDP Port       : 6343
Max. Datagram : 1400 bytes
Time left      : 0 seconds

>
```

Messages: Error: Invalid receiver IP address or failed DNS lookup of hostname.

Command: Set / Show sFlow FlowSampler

Syntax: **sflow flowsampler** [<port_list>] [<sampling_rate>] [<max_hdr_size>]

Description: Set or show flow sampler configuration per port. When operational, the sampling rate 'N' is rounded off to the nearest supported value. The parameters are:

<port_list> : Port list or 'All'. The default is 'All' ports.

<sampling_rate>: Specifies the statistical sampling rate.

The sample rate is specified as N to sample 1/Nth of the packets in the monitored flows. There are no restrictions on the value, but the switch will adjust it to the closest possible sampling rate. Setting to 0 disables sampling.

<max_hdr_size> : Specifies the maximum number of bytes to transmit per flow sample.

The valid range is 14 - 200 bytes. The default is 128 bytes.

```
Example: >sflow flowsampler
Flow Sampler Configuration:
=====

No active flow samplers.
>sflow flowsampler 1 3 14
>sflow flowsampler

Flow Sampler Configuration:
=====

Port   Sampling Rate   Max Hdr
----   -
     1             3           14
>
```

Messages: No active flow samplers.

Note: Sampling rate modified from 100128 to 4096 to cater for H/W limitations

Note: Sampling rate modified from 1001 to 1024 to cater for H/W limitations

Note: Sampling rate modified from 0 to 4096 to cater for H/W limitations

Command: Set / Show sFlow CounterPoller

Syntax: **sflow counterpoller** [<port_list>] [<interval>]

Description: Set or show counter polling interval configuration per port, where:

<port_list>: Port list or 'All'. The default is 'All' ports.

<interval> : Polling interval in the range 0 - 3600. Set to 0 to release this port's resources.

```
Example: >sflow counterpoller

Counter Poller Configuration:
=====

No active counter pollers.
>sflow counterpoller 2 200
>sflow counterpoller 3 300
>sflow counterpoller

Counter Poller Configuration:
=====

Port   Interval
----   -
     2           200
     3           300
>
```

Command: Get / Clear sFlow Statistics Receiver
Syntax: sflow statistics receiver [clear]
Description: Get or clear sFlow receiver statistics, where:
clear: Clear current statistics.

Example: >sflow statistics receiver

```
Receiver Statistics:
=====
Tx Successes   Tx Errors   Flow Samples   Counter Samples
-----
                0             0             0
>
```

Command: sFlow Statistics Samplers
Syntax: sflow statistics samplers [<port_list>] [clear]
Description: Get or clear per-port statistics, where:
<port_list>: Port list or 'All'. The default is 'All' ports.
clear : Clear statistics.

Example: >sflow statistics samplers

```
Per-Port Statistics:
=====
No non-zero counters.
>
>sflow statistics samplers clear
>sflow statistics samplers

Per-Port Statistics:
=====
No non-zero counters.
>sflow statistics samplers 1,2

Per-Port Statistics:
=====

Port   Rx Flow Samples   Tx Flow Samples   Counter Samples
-----
    1             0                 0                 0
    2             0                 0                 0
>
```

VCL Commands

A VLAN Control List (VCL) is used for assigning a particular flow to a particular VLAN. VCLs can enforce VLAN security that is based on a variety of information.

The S3280 VCL (VLAN Control List) commands let you configure the S3280 for MAC-based VLAN, Protocol-based VLAN, and/or IP Subnet-based VLAN mappings.

MAC-based VLAN commands let you add and delete MAC-based VLAN entries and assign the entries to different ports. This page shows only static entries. A MAC address-based VLAN decides the VLAN for forwarding an untagged frame based on the source MAC address of the frame.

Protocol-based VLAN commands let you configure the S3280 for Protocol-to-Group and/or Group-to-VLAN settings. With a protocol-based VLAN, traffic is handled on the basis of its protocol. This basically "segregates" (or forwards) traffic from a port, depending on the particular protocol of that traffic; traffic of any other protocol is not forwarded on the port. For example, it is possible to connect to a given switch:

- a host generating ARP traffic to port 1,
- a network with IPX traffic to port 2, and
- a router forwarding IP traffic to port 3

If a protocol-based VLAN is created that supports IP and contains all three ports, this will prevent IPX traffic from being forwarded to ports 1 and 3, and prevent ARP traffic from being forwarded to ports 2 and 3, but will still allow IP traffic to be forwarded on all three ports.

IP Subnet-based VLAN commands let you define a VLAN membership by the subnet to which a device's IP address belongs. You can add, update, and delete IP subnet-based VLAN entries and assign the entries (membership) to different ports. VLANs are layer 2 constructs, compared with IP subnets which are layer 3 constructs. In an environment employing VLANs, a one-to-one relationship often exists between VLANs and IP subnets, but it is possible to have multiple subnets on one VLAN. VLANs and IP subnets provide independent Layer 2 and Layer 3 constructs that map to each other, and this correspondence helps in network design. Note that this involves only static entries.

The S3280 VCL commands include:

```
>vcl ?
```

Available Commands:

VCL Macvlan Configuration

```
VCL Macvlan Add <mac_addr> <vid> [<port_list>]
```

```
VCL Macvlan Del <mac_addr>
```

```
VCL Status [combined|static|nas|all]
```

```
VCL ProtoVlan Protocol Add Eth2 <ether_type>|arp|ip|ipx|at <group_id>
```

```
VCL ProtoVlan Protocol Add Snap <oui>|rfc_1042|snap_8021h <pid> <group_id>
```

```
VCL ProtoVlan Protocol Add Llc <dsap> <ssap> <group_id>
```

```
VCL ProtoVlan Protocol Delete Eth2 <ether_type>|arp|ip|ipx|at
```

```
VCL ProtoVlan Protocol Delete Snap <oui>|rfc_1042|snap_8021h <pid>
```

```
VCL ProtoVlan Protocol Delete Llc <dsap> <ssap>
```

```
VCL ProtoVlan Vlan Add [<port_list>] <group_id> <vid>
```

```
VCL ProtoVlan Vlan Delete [<port_list>] <group_id>
```

VCL ProtoVlan Conf

```
VCL IPVlan Configuration [<vce_id>]
```

```
VCL IPVlan Add [<vce_id>] <ip_addr_mask> <vid> [<port_list>]
```

```
VCL IPVlan Delete <vce_id>
```

```
>
```

Note: Protocol-based VLANs and IP Subnet-based VLANs work only on untagged and priority tagged frames, while MAC based VLANs work on all kinds of frames.

The S3280 sFlow commands are explained below.

Command: Show VCL MAC VLAN Configuration
Syntax: **vcl macvlan config**
Description: Show the existing VCL MAC-based VLAN configuration.
Example: **>vcl macvlan con**

```
MAC Address          VID    Ports
-----
00-00-00-00-00-00  100    4
>
```

Command: Add / Change VCL MAC VLAN Entry
Syntax: **vcl macvlan add <mac_addr> <vid> [<port_list>]**
Description: Add or modify VCL MAC-based VLAN entry. The parameters are:
<mac_addr> : MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', where x is a hexadecimal digit) .
<vid> : VLAN ID (1-4094).
<port_list>: Port list or 'All'. The default is 'All' ports.

Example: **>vcl macvlan config**
>vcl macvlan add 00-00-00-00-00-00 100
>vcl macvlan config

```
MAC Address          VID    Ports
-----
00-00-00-00-00-00  100    1-10
>
```

Messages: **>vcl macvlan add 11-22-33-44-55-66 2 1,2,3**
cli_cmd_vcl_macvlan_add: Error while adding MAC-based VLAN entry

Command: Delete VCL MAC VLAN Entry
Syntax: **vcl macvlan del <mac_addr>**
Description: Delete an existing VCL MAC-based VLAN entry, where:
<mac_addr>: MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', where x is a hexadecimal digit).

Example: **>vcl macvlan del 11-22-33-44-55-66**
 Deletion failed
>vcl macvlan conf

```
MAC Address          VID    Ports
-----
00-00-00-00-00-00  100    1-13
00-00-77-00-8d-0f  10     1-13
>vcl macvlan del 00-00-00-00-00-00
>vcl macvlan conf

MAC Address          VID    Ports
-----
00-00-77-00-8d-0f  10     1-13
>
```

Command: Show VCL Status

Syntax: vcl status [combined|static|nas|all]

Description: Display existing VCL MAC-based VLAN users configuration, where: **combined|static|nas|all**: VCL User configuration to display.

Example: >vcl status

```

Entry   VCL MAC User   MAC Address           VID   Ports
-----
1       Static         00-00-00-00-00-00    1     3-5,9
        Combined     00-00-00-00-00-00    1     3-5,9
>

```

Command: Add VCL ProtoVLAN Protocol Eth2

Syntax: vcl protovlan protocol add eth2 <ether_type>|arp|ip|ipx|at <group_id>

Description: Add VCL protocol-based VLAN Ethernet-II protocol-to-group mapping, where: <ether_type>|arp|ip|ipx|at: an Ether Type in the range of 0x0600 - 0xFFFF.

arp : use 0x0806 - ARP (Address Resolution Protocol)
ip : use 0x0800 - IP (Internet Protocol)
ipx : use 0x8137 - IPX (Internet Packet Exchange)
at : use 0x88A2 - ATA over Ethernet

<group_id> : Protocol group ID.

Example: >vcl protovlan protocol add eth2 ip 1
>

Command: Add VCL ProtoVLAN Protocol SNAP

Syntax: vcl protovlan protocol add snap <oui>|rfc_1042|snap_8021h <pid> <group_id>

Description: Add VCL protocol-based VLAN SNAP protocol to group mapping, where:

<oui>|rfc_1042|snap_8021h: OUI value (Hexadecimal 00-00-00 to FF-FF-FF).

oui : organizationally unique identifier in the format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.

rfc_1042 : use IETF RFC 1042 as the method of encapsulating the Internet Protocol (IP) datagrams and Address Resolution Protocol (ARP) requests.

snap_8021h : Set the encapsulation transformation method to 802.1h (the default setting).

<pid> : PID value (0x0-0xFFFF). If OUI is 00-00-00, valid range of PID is from 0x0600 - 0xFFFF.

<group_id> : Protocol group ID.

Example: >vcl protovlan protocol add snap 11-22-33 0x800 1
>

Command: Add VCL ProtoVlan Protocol LLC

Syntax: vcl protovlan protocol add llc <dsap> <ssap> <group_id>

Description: Add VCL protocol-based VLAN LLC protocol-to-group mapping, where:

<dsap> : DSAP value (0x00-0xFF). The DSAP is the Destination Service Access Point.

<ssap> : SSAP value (0x00-0xFF). The SSAP is the Source Service Access Point.

<group_id>: Protocol group ID.

Example: >vcl protovlan protocol add llc 0x11 0x22 1
>

Command: Delete VCL ProtoVLAN Protocol Eth2

Syntax: vcl protovlan protocol delete eth2 <ether_type>|arp|ip|ipx|at>

Description: Delete an existing VCL protocol-based VLAN Ethernet-II protocol from the group mapping. The parameters are:
<ether_type>|arp|ip|ipx|at: Ether Type (0x0600 - 0xFFFF).

Example:

```
>VCL ProtoVlan Conf
Protocol Type Protocol (Value) Group ID
-----
LLC_Other DSAP:0x11; SSAP:0x22 1
LLC_SNAP OUI-11:22:33; PID:0x800 1
EthernetII ETYPE:0x900 1

>vcl protovlan protocol delete eth2 0x900
>VCL ProtoVlan Conf
Protocol Type Protocol (Value) Group ID
-----
LLC_Other DSAP:0x11; SSAP:0x22 1
LLC_SNAP OUI-11:22:33; PID:0x800 1

>
```

The SSAP is the Source Service Access Point and the DSAP is the Destination Service Access Point.

Command: **Delete VCL Proto VLAN Protocol SNAP Mapping**

Syntax: **vcl protovlan protocol delete snap <oui>|rfc_1042|snap_8021h <pid>**

Description: Delete VCL protocol-based VLAN SNAP protocol to group mapping. The parameters are:
<oui>|rfc_1042|snap_8021h: OUI value (Hexadecimal 00-00-00 to FF-FF-FF).

oui: : Organizationally unique identifier in the format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.

rfc_1042 : Use IETF RFC 1042 as the method of encapsulating the Internet Protocol (IP) datagrams and Address Resolution Protocol (ARP) requests.

snap_8021h : Set the encapsulation transformation method to 802.1h (the default setting).

<pid> : PID value (0x0-0xFFFF). If OUI is 00-00-00, valid range of PID is from 0x0600-0xFFFF.

Example:

```
>vcl protovlan protocol delete snap 11-22-33 0x900
>
```

Messages: *Deleting Protocol to Group mapping Failed*

Command: **Delete VCL ProtoVlan Protocol LLC**

Syntax: **vcl protovlan protocol delete llc <dsap> <ssap>**

Description: Delete VCL protocol-based VLAN LLC protocol-to-group mapping. The parameters are:
<dsap>: DSAP value (0x00-0xFF).
<ssap>: SSAP value (0x00-0xFF).

Example:

```
>vcl protovlan protocol delete llc 1 2
>
```

Messages: *Deleting Protocol to Group mapping Failed*

Command: Add VCL ProtoVlan VLAN

Syntax: `vcl protovlan vlan add` [<port_list>] <group_id> <vid>

Description: Add VCL protocol-based VLAN group-to-VLAN mapping, where:
 <port_list>: Port list or 'all'; the default is 'All' ports.
 <group_id> : Protocol group ID.
 <vid> : VLAN ID (1-4094).

Example:

```
>vcl protovlan vlan add 1 1 1
>
```

Command: Delete VCL ProtoVlan VLAN

Syntax: `vcl protovlan vlan delete` [<port_list>] <group_id>

Description: Delete VCL protocol-based VLAN group-to-VLAN mapping, where:
 <port_list>: Port list or 'all'. the default is 'All' ports.
 <group_id> : Protocol group ID.

Example:

```
>vcl protovlan vlan delete 1 1
>
```

Command: VCL ProtoVlan Configuration

Syntax: `vcl protovlan vlan conf`

Description: Show VCL protocol-based VLAN entries.

Example 1:

```
>VCL ProtoVlan Conf
Protocol Type Protocol (Value) Group ID
-----
LLC_Other DSAP:0x11; SSAP:0x22 1
LLC_SNAP OUI-11:22:33; PID:0x800 1
EthernetII ETYPE:0x900 1

>
```

Example 2:

```
>vcl pro con
Protocol Type Protocol (Value) Group ID
-----
LLC_Other DSAP:0xff; SSAP:0xff s2grp
LLC_SNAP OUI-00:e0:2b; PID:0x1 sgrp
EthernetII ETYPE:0x800 etype0x800

Group ID VID Ports
-----
sgrp2 20 4

>
```

The SSAP is the Source Service Access Point and the DSAP is the Destination Service Access Point.

Command: Show VCL IPvlan Configuration

Syntax: vcl ipvlan config [<vce_id>]

Description: Displays the current VCL IP Subnet-based VLAN configuration, where:
<vce_id>: Unique VCE ID for each VCL entry.

Example 1: The default display:

```
>vcl ipvlan config
VCE ID  IP Address      Mask Length  VID  Ports
-----  -
>
```

Example 2: A configured display:

```
>vcl ipvlan config
VCE ID  IP Address      Mask Length  VID  Ports
-----  -
1       192.168.1.30   24           1    1-3,8
2       192.168.1.30   24           1    1,2,6,8
3       192.168.1.40   24           2    1,2,6
>
```

Messages: Entry with VCE ID 1 not found

Command: Add / Modify VCL IP VLAN

Syntax: vcl ipvlan add [<vce_id>] <ip_addr_mask> <vid> [<port_list>]

Description: Add a new or modify an existing VCL IP Subnet-based VLAN entry. IP subnet-based VLAN entries can be configured from the CLI. With this method, a VLAN membership is defined by the subnet to which a device's IP address belongs. This command lets you add a new IP subnet-based VLAN entry and assign port members. VLANs are layer 2 constructs, compared with IP subnets which are layer 3 constructs. In an environment employing VLANs, a one-to-one relationship often exists between VLANs and IP subnets, but it is possible to have multiple subnets on one VLAN. VLANs and IP subnets provide independent Layer 2 and Layer 3 constructs that map to each other, and this correspondence helps in network design. Note that this command adds/edits only static entries. The parameters are:

<vce_id> : A unique VCE ID for each VCL entry

<ip_addr_mask>: Source IP address and mask (Format: a.b.c.d/n). Enter a valid IP address in dotted decimal notation ('x.y.z.w') where x, y, and z are decimal numbers from 0 to 255, and the mask length is from 1-32.

<vid> : VLAN ID (1-4094) of an existing VLAN.

<port_list> : Port list or 'All'. The default is 'All' ports (1-8).

Example:

```
>vcl ipvlan add 1 192.168.1.30/24 1 1,2,3,8
>vcl ipvlan add 2 192.168.1.30/24 1 1,2,6,8
>vcl ipvlan add 3 192.168.1.40/24 2 1,2,6
>vcl ipvlan config
VCE ID  IP Address      Mask Length  VID  Ports
-----  -
1       192.168.1.30   24           1    1-3,8
2       192.168.1.30   24           1    1,2,6,8
3       192.168.1.40   24           2    1,2,6
>
```

Messages: Add failed. IP Subnet-based VLAN entry already configured with different subnet

Command: Delete VCL IPvlan

Syntax: `vcl ipvlan delete <vce_id>`

Description: Delete one or more existing IP subnet-based VLAN entries and their assigned port memberships.

Example:

```
>vcl ipvlan delete 1
>vcl ipvlan delete 2
>vcl ipvlan delete 3
>vcl ipvlan config
>
```

Messages: *IP Subnet-based VLAN deletion failed - matching entry not found*

EtherSAT Loopback Configuration Commands (S3280-TST Only)

See the RFC2544 Performance Tests User Guide, 33540 for the EtherSAT Loopback configuration commands.

Note: The S3280-TST models have an FPGA Assist board built in to offload processing for certain functions specific to the S3280-TST (i.e., that are not available on the S3280 model). These commands can only be used with the S3280-TST model.

Static Routing (SIR) Commands (S3280-TST Only)

See the Static IP Routing (SIR) User Guide, 33542 for the SIR (Static IP Routing) commands.

The Static IP Routing (SIR) feature provides routing capabilities for up to 16 L3 endpoints. The routing is based on statically configured routes. Up to 128 static routes can be stored in the routing tables. The SIR feature lets you define L3 routing endpoints over the VLANs configured in the NID. Through such endpoints, the traffic is routed between the VLANs, such as hosts from one VLAN can communicate through hosts located in different VLANs.

Troubleshooting

1. Check the S3280 Back Panel Connections (see the S3280 Install Guide).
2. Verify the Installation. Check the Operating System, Web Browser, Telnet Client, and/or Terminal Emulation package support (see the S3280 Install Guide).
3. Make sure your particular model supports the function attempted.
4. Check the S3280 (or -TST) front panel connectors and LEDs; see the S3280 or S3280-TST Install Guide.
5. Respond to any S3280 CLI error messages (see below).
6. Run the S3280 Diagnostics tests and verification functions (e.g., EtherSAT Loopback, Ping, VeriPHY). See the related section of this manual or the “Diagnostics” sub-menu section in the S3280 User Guide.
7. Perform the S3280 troubleshooting and service functions (e.g., Restart Device, reset to Factory Defaults, Software Upload, Image Select). See the “Maintenance” section in the S3280 User Guide.
8. Check the S3280 operating parameters (e.g., Information, CPU Load, Log, Detailed Log). See the “Monitor” section in the S3280 User Guide.
9. See the related manual for troubleshooting advanced features such as Static IP Routing (SIR) or EtherSAT Loopback.

Messages and Recovery

The S3280 displays error and information messages from the CLI and Web interface. This section lists the CLI messages, provides examples, and discusses the message meaning of and possible recovery steps. For web interface messages, refer to the S3280 Web Interface User Guide manual.

For many messages, recovery involves reviewing the command/function description and verifying the entry selection/syntax. For example, for many CLI messages, the first recovery step would be to refer to the applicable Command section (e.g., “System” or “IP” or “Ports”) or the related CLI Command Group or specific CLI command for syntax /instructions.

For any error condition, you can check the [TN Tech Support web](#) site for possible solutions. For any problem that persists, contact TN Tech Support in the US or Canada at 1-800-260-1312, International at 00-1-952-941-7600; via fax at +1 952-941-2322; or via Email at techsupport@transition.com.

Basic Recovery Steps

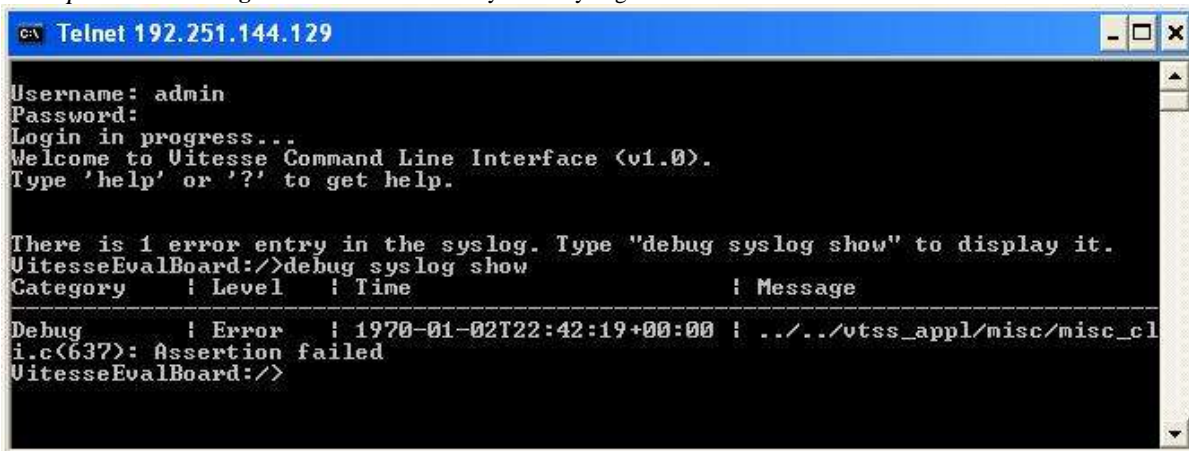
You entered a command, but the operation failed or is still in process.

1. Wait for a few moments for the operation to complete.
2. Use the **Help** or **?** command to get assistance (help) on a group of commands or on a specific command.
3. Make sure this is the command you want and that the device/port/configuration supports this command.
4. Make sure this device/port supports the function attempted. Use the **go** command to switch locations.
5. Verify the command syntax and re-enter the command. See the related section of the manual for specifics.
6. Try using the Web interface to perform the function.
7. If the “continue **y**(es) **n**(o) prompt” displays, type **y** and press **Enter** to continue.
8. If the problem persists, contact TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600; [TN Tech Support web](#); fax: +1 952-941-2322; Email: techsupport@transition.com.

CLI Messages

Message: There is 1 error entry in the syslog - Assertion failed

Example: Telnet > Login > There is 1 error entry in the syslog



```

C:\ Telnet 192.251.144.129
Username: admin
Password:
Login in progress...
Welcome to Uitesse Command Line Interface (v1.0).
Type 'help' or '?' to get help.

There is 1 error entry in the syslog. Type "debug syslog show" to display it.
UitesseEvalBoard:/>debug syslog show
Category      | Level  | Time                               | Message
-----
Debug         | Error  | 1970-01-02T22:42:19+00:00 | ../../vtss_appl/misc/misc_cl
i.c(637): Assertion failed
UitesseEvalBoard:/>

```

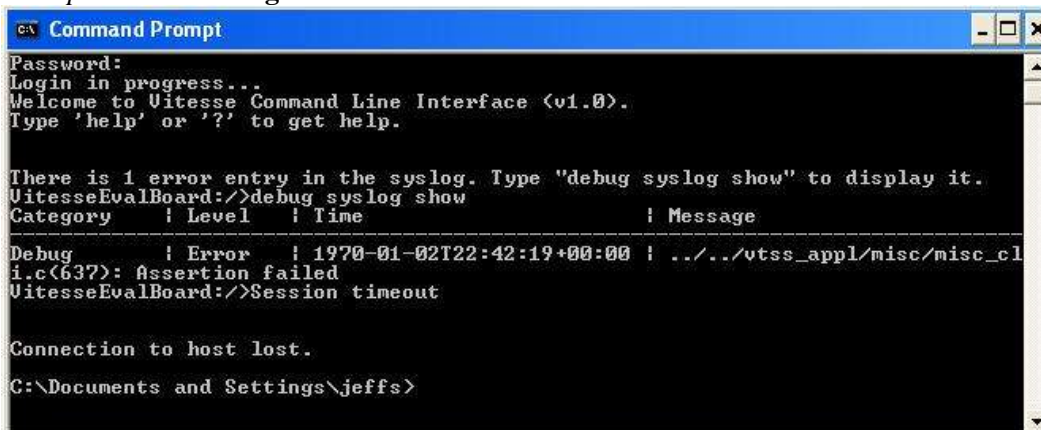
Meaning: You logged in successfully, an error occurred and this message displayed.

Recovery:

1. Follow the on-screen prompts to display the error, or press **Enter** to display the commands Help screen.
2. If the problem persists, contact TN Tech Support.

Message: Session timeout - Connection to host lost

Example: Telnet > Login > 1 error > Session timeout - Connection to host lost:



```

C:\ Command Prompt
Password:
Login in progress...
Welcome to Uitesse Command Line Interface (v1.0).
Type 'help' or '?' to get help.

There is 1 error entry in the syslog. Type "debug syslog show" to display it.
UitesseEvalBoard:/>debug syslog show
Category      | Level  | Time                               | Message
-----
Debug         | Error  | 1970-01-02T22:42:19+00:00 | ../../vtss_appl/misc/misc_cl
i.c(637): Assertion failed
UitesseEvalBoard:/>Session timeout

Connection to host lost.
C:\Documents and Settings\jeffs>

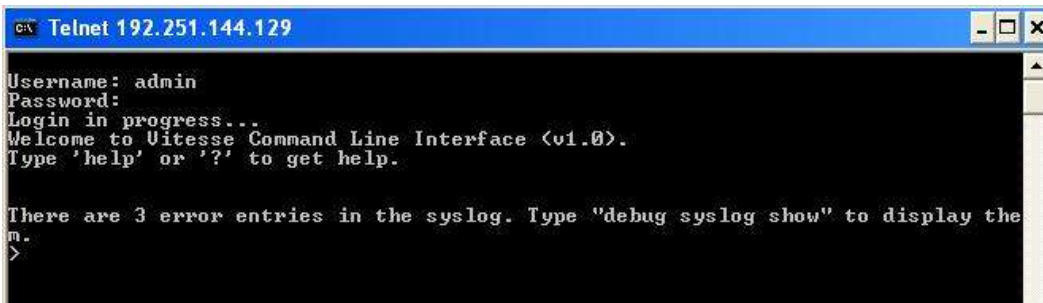
```

Meaning: You logged in successfully, an error occurred, this message displayed, and the Telnet connection dropped.

Recovery:

1. Log in via Telnet again.
2. If the problem persists, contact TN Tech Support.

Message: There are 3 error entries in the syslog. Type “debug syslog show” to display them.



```

c:\ Telnet 192.251.144.129
Username: admin
Password:
Login in progress...
Welcome to Uitesse Command Line Interface (v1.0).
Type 'help' or '?' to get help.

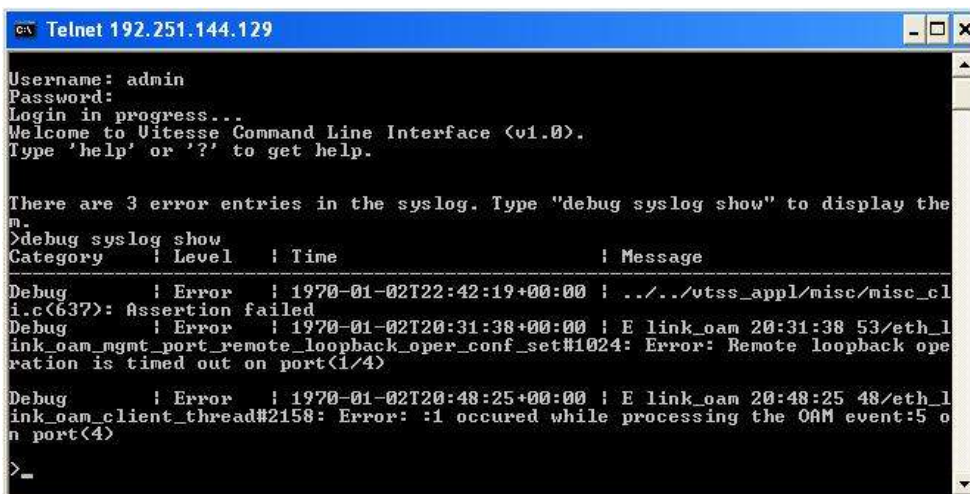
There are 3 error entries in the syslog. Type "debug syslog show" to display the
m.
>

```

Meaning: Startup message - information only.

Recovery:

1. You can either type the command “**debug syslog show**” and press **Enter** to display the error entries, or just press the **Enter** key to continue without addressing the error entries.



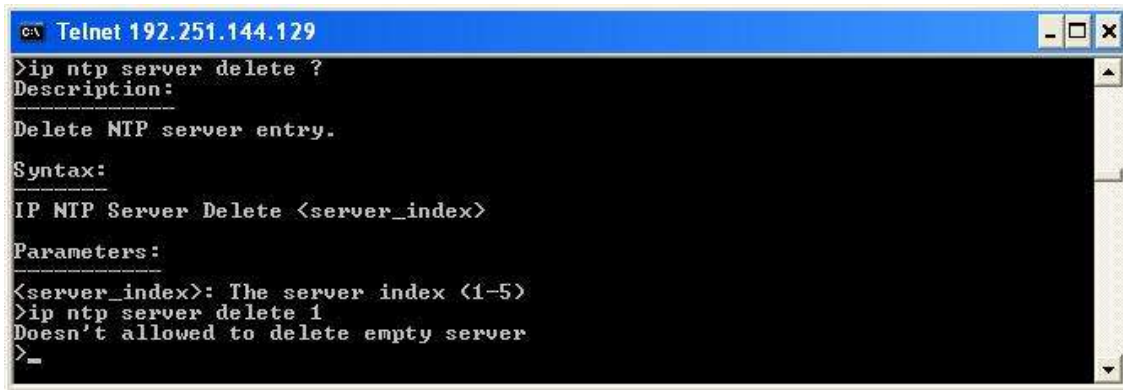
```

c:\ Telnet 192.251.144.129
Username: admin
Password:
Login in progress...
Welcome to Uitesse Command Line Interface (v1.0).
Type 'help' or '?' to get help.

There are 3 error entries in the syslog. Type "debug syslog show" to display the
m.
>debug syslog show
Category    | Level    | Time                               | Message
-----
Debug      | Error    | 1970-01-02T22:42:19+00:00 | ../../vtss_appl/misc/misc_cl
i.c(637): Assertion failed
Debug      | Error    | 1970-01-02T20:31:38+00:00 | E link_oam 20:31:38 53/eth_1
ink_oam_mgmt_port_remote_loopback_oper_conf_set#1024: Error: Remote loopback ope
ration is timed out on port<1/4>
Debug      | Error    | 1970-01-02T20:48:25+00:00 | E link_oam 20:48:25 48/eth_1
ink_oam_client_thread#2158: Error: :1 occurred while processing the OAM event:5 o
n port<4>
>_

```

3. If the problem persists, contact TN Tech Support.

Message: Doesn't allowed to delete empty server


```

C:\> Telnet 192.251.144.129
>ip ntp server delete ?
Description:
-----
Delete NTP server entry.
Syntax:
-----
IP NTP Server Delete <server_index>
Parameters:
-----
<server_index>: The server index (1-5)
>ip ntp server delete 1
Doesn't allowed to delete empty server
>_

```

Meaning: You entered a command to delete a specific NTP Server, but that NTP Server has not been created or does not exist.

Recovery:

1. Make sure the NTP Server you want to delete has been created and has not yet been deleted.
2. Retry the IP>**ntp server delete x** command with r a valid server index (1-5).
3. If the problem persists, contact TN Tech Support.

Message: Port x does not support this mode


```

>port mode auto
>port mode 100hdx
Port 9 does not support this mode
Port 10 does not support this mode
>

```

Meaning: Error message displays if the entered port number does not support the selected mode.

Recovery:

1. Verify the command syntax (**port mode** [<port_list>] [auto|10hdx|10fdx|100hdx|100fdx|1000fdx|2500fdx]).
2. Type **port mode** and press **Enter** to display the port / mode / list table.
3. Retry the command.
4. If the problem persists, contact TN Tech Support.

Message: Port 2 is already included in aggregation 2

Meaning: You tried to aggregate a port in more than one Aggregation ID.

Recovery:

1. Re-enter the “Aggr Add” command with the correct parameters.
2. See the related command section for specific information.

Message: Port x is already included in a static aggregation

Example:

```

LACP>mode 1,2,3 enable
Port 2 is already included in a static aggregation
Port 3 is already included in a static aggregation
LACP>

```

Meaning: The LACP mode command entry failed for one or more particular ports.

Recovery:

1. Re-enter the “lACP mode” command with the correct parameters.
2. See the “lACP mode” command section for specific information.

Message: Please disable trap security engine ID probe first

Example: >**security switch snmp trap security engine id 800007e5017f000001**

Please disable trap security engine ID probe first

Meaning: You entered a command before the system can accept its parameter.

Recovery:

1. Disable the trap security engine ID probe before using this command.
2. See the “Set or Show SNMP Trap Probe Security Engine ID“ command description.

Message: **tftp client put failed: 8**

Example: >**config backup binary 192.168.1.30 S3280_v0.2.0_conf.bin**

tftp client put failed: 8

>

Meaning: The backup procedure failed, likely because of an unsupported TFTP Server product or version. For example, SolarWinds Multi-Threaded TFTP Server for Windows Version 8.2.7 (Standard Edition) does not function with the S3280 **config backup binary** command.

SolarWinds TFTP Server version 8.2.7 (September 2005) does not work. SolarWinds TFTP server version 10.4.0.14 works fine for S3280 binary backups.

Recovery:

1. If using SolarWinds Standard Edition v 8.2.7, uninstall it and download and install the latest version.
2. Configure and start the new version and retry the S3280 **config backup binary** command.

Message:

Cannot find the module name. module ID = x

Change to lower privilege level will lock yourself out.

The privilege level of x is y.

Meaning: A user privilege level issue occurred.

Recovery:

1. Re-enter the command with a different privilege level.
2. See the “[Security Switch Privilege](#)” command on page 61.

Message: **W web 12:58:34 61/handler_config_https_cert_load#272: Warning: Please disable HTTPS mode first**

Meaning: An HTTPS security certificate loading issue occurred requiring HTTPS to be disabled.

Recovery:

1. Disable HTTPS. See the “[Security Switch Commands](#)” on page 76.

Message: **No port members for VLAN "vid". Please check the delete button to delete VLAN from the list or add the members.**

Meaning: You tried to delete a non-existent VLAN translation entry from a group.

1. Re-enter the command with a different (existing) group.
2. Add port member to the group and re-try the operation.
3. Make sure you are not trying to delete VLAN 1. Deleting VLAN 1 causes issues with forwarding.
4. To make sure no ports belong to VLAN 1, then add VLAN 1 with all ports in the forbidden state.
5. See the **Delete VLAN Translation Group Entry** command for more information.

Message: **tftp client get failed: 8**

Example: >**config restore binary 192.168.1.30 S3280_v0.1.0_conf.bin**

tftp client get failed: 8


```
>config restore binary 192.168.1.30 S3280_v0.3.0_conf.bin
Restore successful
```

Meaning: The Configuration Restore Binary command (*tftp get*) failed.

Recovery:

1. Make sure the TFTP server is configured and running.
2. Make sure the file name is accurate and located properly.
3. See the “[config restore binary](#)” command on page 18.

Problem: Policing on ECE traffic on UNI doesn’t seem to work

Meaning: At the **Configuration > EVC** menu path, you:

1. Created an EVPL service and assigned a policer to one of the UNI ECEs.
2. Configured an EVPL as shown below:

EVC ID	VID	IVID	Learning	NNI Ports	Inner Type/Mode/VID	Inner PCP/DEI	Outer VID
2	55	111	Disabled	4	None/Normal/0	Fixed 0/0	0

ECE ID	Direction	EVC ID	Tag Type	VID	PCP	DEI	Frame	UNI Ports
2	Both	2	Tagged	10	Any	Any	Any	2
3	Both	2	Tagged	11	Any	Any	Any	2

3. Configured an ECE (ECE ID: 2) with Policy Number: 1 (Policer assigned).
4. Configured Policer (Policer=1, State=enabled, Mode=Aware, CIR=5000, CBS=64000, EIR=1.EBS=0).
5. When frames with VLAN Id = 10 are sent to the UNI Port 2, its not rate limited to 5k, but is to the line rate. The coupling between a policer and an ECE is done in the ACL configuration. You must add an ACE with the policy specified in the ECE. This is done by the CLI command "**Security/Network/ACL>add 1 policy 1 0xf any disable 1**". This command will add ACE ID 2 with policy 1 and it will accept all VLANs; rate limiting is disable and the EVC policer is 1.

In other words, the ECE will filter on the VLAN ID specified for the UNI. This is done in IS1 TCAM, and the next step is the policing done by ACE in IS2.

Note that the policer it self is always colour aware (aware or coupled). If you want colour-blind policing, you can use QCL classification to make all traffic green.

Recovery:

1. Create an EVPL EVC and assign a policer to the ECE on Port 2 (UNI) for ingress bandwidth limiting (see command sequence below).
2. Send traffic at line rate; there will be no rate limits on the UNI.

Command sequence:

```
>evc conf
Port  DEI Mode  Tag Mode  Address
----  -
1     Fixed  Outer    SMAC/SIP
2     Fixed  Outer    SMAC/SIP
3     Fixed  Outer    SMAC/SIP
4     Fixed  Outer    SMAC/SIP
5     Fixed  Outer    SMAC/SIP
6     Fixed  Outer    SMAC/SIP
7     Fixed  Outer    SMAC/SIP
8     Fixed  Outer    SMAC/SIP
9     Fixed  Outer    SMAC/SIP

Policer  State  Mode  CIR  CBS  EIR  EBS
-----  -
1        Enabled  Aware  5000  64000  0  0      <== Policier created
2        Disabled  Aware  0  0  0  0
3        Disabled  Aware  0  0  0  0
```

4	Disabled	Aware	0	0	0	0
5	Disabled	Aware	0	0	0	0
6	Disabled	Aware	0	0	0	0
7	Disabled	Aware	0	0	0	0
8	Disabled	Aware	0	0	0	0
9	Disabled	Aware	0	0	0	0
10	Disabled	Aware	0	0	0	0
:						
:						
125	Disabled	Aware	0	0	0	0
126	Disabled	Aware	0	0	0	0
127	Disabled	Aware	0	0	0	0
128	Disabled	Aware	0	0	0	0

EVC ID	VID	IVID	Learning	NNI Ports	Inner Type/Mode/VID	Inner PCP/DEI	Outer VID
2	55	111	Disabled	4	None/Normal/0	Fixed	0/0 0

ECE ID	Direction	EVC ID	Tag Type	VID	PCP	DEI	Frame	UNI Ports
2	Both	2	Tagged	10	Any	Any	Any	2
3	Both	2	Tagged	11	Any	Any	Any	2

>evc ece status 2

ECE ID : 2

Key Parameters

```

-----
UNI Ports : 2
DMAC Type : Any
SMAC : Any
Outer Tag Type : Tagged
Outer VID : 10
Outer PCP : Any
Outer DEI : Any
Frame Type : Any
    
```

Action Parameters

```

-----
Direction : Both
EVC ID : 2
Tag Pop Count : 0
Policy Number : 1 <== Policer assigned to ECE
Class : Disabled
Outer Mode : Disabled
Outer PCP/DEI : Fixed
Outer PCP : 0
Outer DEI : 0
Conflict : No
>
    
```

```

>evc ece status 3
ECE ID          : 3

Key Parameters
-----
UNI Ports      : 2
DMAC Type     : Any
SMAC          : Any
Outer Tag Type : Tagged
Outer VID     : 11
Outer PCP     : Any
Outer DEI     : Any
Frame Type    : Any

Action Parameters
-----
Direction     : Both
EVC ID       : 2

Tag Pop Count : 0
Policy Number : 0
Class        : Disabled
Outer Mode   : Disabled
Outer PCP/DEI : Fixed
Outer PCP    : 0
Outer DEI    : 0
Conflict     : No
>
>evc policer 1
Policer  State      Mode      CIR      CBS      EIR      EBS
-----  -
1         Enabled    Aware    5000    64000   0        0

```

Messages:

%s User Configured a different VID on the ports

Error: VLAN is configured by Static VLAN user. Check VLAN LOOKUP info. Operation aborted.

Invalid parameter: x

Missing <vid><name> parameter

VLAN deletion failure

VLAN Id Membership conflict

VLAN table configuration open error

VLAN table full

Meaning: A VLAN Forbidden conflict or error occurred, or you tried to modify or delete a non-existent VLAN.

Recovery:

1. Verify the command parameters.
2. See the “[VLAN Commands](#)” on page 57.

Message: Invalid parameter xxxx

Meaning: The command you entered was not accepted because a parameter entry was outside the valid range.

Recovery:

1. Check the **xxxx** portion of the command for possible meaning in understanding the cause of the problem.
2. Use the show version of the command if available.
3. Check the command syntax; see the related command page and re-enter the command.

Examples: An "Invalid parameter" message displays if you try to enter a value outside of the valid range of 1518-9600 packets (e.g., Invalid parameter: 9999 displays). Examples are provided below.

```
>security switch snmp trap version 2x
Invalid parameter: 2x

>security switch snmp user add
Invalid parameter: sha

>security network acl rate 1,2 kbps 3*100
Invalid parameter: 3*100

>security network acl add 1 2 3 4 5 6 7 8 9
Invalid parameter: 8

STP>maxhops 5
Invalid parameter: 5

STP>maxage 4
Invalid parameter: 4
<max age>: STP maximum age time (6-40) ** s/b 6-39

>LLDP Optional TLV all sys1 engsyst opttlvenabl 192.168.1.110 enable
Invalid parameter: sys1

>lldp delay 11
Delay must be less than 1/4 of Interval

>evc ece add 1 1 1 1 unicast any T tagged 1 1 1 A 4 1 any 1 fragment any any 6 any D nni-to-uni V 1 P 1
1 1 1 K 1 O enable fixed 1 1
Invalid parameter: unicast

>evc ece delete 1
W evc 04:37:12 50/evc_mgmt_ece_del#1297: Warning: id: 1 not found
ECE delete failed

>eps create 1 domport lpl w p w p aps enable
Invalid parameter: w

MEP>config 1 mip ingress 1 domport 5 itu megidl 1 1 1 enable
Invalid parameter error returned from MEP

MEP>ais config 1 2 lm clear enable
Invalid parameter error returned from MEP

MEP>lck config 1 2 ls enable
Invalid parameter error returned from MEP

QoS>port queueshaper rate 1 4 6660000
Invalid parameter: 6660000

QoS>qcl add 1 last 1 tag 1 0-1 any any unicast kw1 0x900 1 any any any k any any k any any EF yes any
any k any 1 0 BE
Invalid parameter: last

QoS>qcl lookup all
Invalid parameter: all

>ipmc router 1 enable mld
Invalid parameter: mld
```

Message: No port members for VLAN "vid". Please check the delete button to delete VLAN from the list or add the members.

Meaning: You tried to delete a non-existing VLAN translation entry from a group.

Recovery:

1. Follow the on-screen instructions.
2. See the [vlan translation delete](#) command on page 45.

Message: The privilege level of 'Read-only' should be less than or equal to 'Read-write'

Meaning: The security privilege level entered was rejected by the CLI. For example:

```
>security switch privilege level group ptp 1
The privilege level of 'Read-only' should be less than or equal to 'Read-write'
>security switch privilege level group ptp 15
The privilege level of 'Read-only' should be less than or equal to 'Read-write'
>
```

Recovery:

1. Re-enter a valid security privilege level.
2. See the [security switch privilege level group](#) command on page 60.

Message: >W web 08:14:26 53/handler_config_https_cert_load#258: Warning: SSL Certificate PEM file size too big

Meaning: The HTTPS certificate had a problem loading.

Recovery:

1. Verify the certificate's file type and file size and re-try the command.
2. See the [security switch https cert show](#) command on page 62.

Message:

Error: File S3280-cacert-key.pem was not found

Error: Please disable HTTPS mode first

Meaning: You must disable HTTPS mode before using this command.

Recovery:

1. Disable HTTPS mode before using this command (see the "Security Switch HTTPS Mode" command).
2. See the "[Security Switch HTTPS Group](#)" commands on pages 63-65.
3. Re-try the failed command.

Message:

Invalid <oid_subtree> parameter: xxxx
Invalid parameter: 80
Invalid parameter: sha
Invalid <engineid> parameter: 123456789
The entry 'xxxxxxx' is not exist
The format of 'Engine ID' may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string
The group name 'xxxx' is not exist
The length is restricted to 8 - 40
The security name 'xxxx' is not exist
Trap security engine ID should not NULL

Meaning: An SNMP parameter entry failed.

Recovery:

1. Use the “show” version of the commands and verify the correct syntax.
2. See the “[Security Switch SNMP Group](#)” commands section on page 78.

Message:

<data_source> dosen't exit
Invalid <history_id> parameter: 0
Invalid <rising_threshold> parameter: -2

Meaning: An RMON parameter entry failed.

Recovery:

1. Use the “show” version of the commands and verify the correct syntax.
2. See the “[Security Switch RMON Group Commands](#)” on pages 70-74.

Messages:

ACL Delete failed
E api/cil 03:51:14 31/126_acl_policer_free#5997: Error: policer 0 already free
Invalid <ace_id> parameter: 0
Invalid parameter: 3*100

Meaning:

Recovery:

1. Use the “show” version of the commands and verify the correct syntax.
2. See the “[Security Network ACL Group](#)” commands on pages 99-102.

Message: We need at least one server

Meaning: You tried to set or show the DHCP relay mode without at least one DHCP server enabled and configured.

Recovery:

1. Enable and configure one or more DHCP servers and retry the command.
2. See the “[Security Network DHCP Group](#)” commands on pages 105-107.

*Message:***Port x is already included in aggregation x
The aggregation does not exist**

Meaning: You tried to aggregate a port in more than one Aggregation ID, or you tried to delete a non-existent aggregation.

Recovery:

1. Use the “show” version of the Aggregation commands or the ‘aggr lookup’ command to verify the correct syntax of <aggr_id>.
2. Try deleting another aggregation. See the “[aggregation add](#)” command on page 141.
3. Try adding a different aggregation. See the “[aggregation delete](#)” command on page 142.

Message: Port x is already included in a static aggregation

Meaning: You tried to set or display the LACP Role or the LACP Key, but one already exists.

Recovery:

1. See the ‘[LACP Key](#)’ command on page 144.
2. See the ‘[LACP Role](#)’ command on page 145.

Message: No LLDP entries found

Meaning: You entered an “lldp info” command to display existing (configured) LLDP neighbor device information, but no LLDP neighbors exist.

Recovery:

1. Make sure one or more neighbor devices are configured.
2. Verify the <port_list> parameter entered.
3. See the “[LLDP Commands](#)” on pages 147-152.

Message: No LLDP-MED entries found

Meaning: You entered the “lldpmed info” command to show LLDP-MED neighbor device information, but no LLDP-MED neighbors exist.

Recovery:

1. Make sure one or more neighbor devices are configured.
2. Verify the <port_list> parameter entered.
3. See the “[lldpmed info](#)” command on page 153.

Message: EVC x does not exist

Meaning: You entered an “EVC Lookup” or “EVC Delete” command but the specified EVC does not exist.

Recovery:

1. Verify that an existing EVC ID (1-128) exists.
2. Create a new EVC if required.
3. Retry the command with a proper <evc_id> parameter entry. See the “[evc lookup](#)” or “[evc delete](#)” commands on pages 166-168.

Message: Invalid parameter: w

Meaning: You entered an **eps create** command, but the command failed.

Recovery:

1. Use the “**eps state**” command to verify the current state.
2. See the “[EPS Create](#)” command on page [171](#) for specific parameter requirements.

Message: Operating on an instance not created

Meaning: You entered an **eps** command, but the instance requested does not yet exist.

Recovery:

1. Use the **eps state** command to verify the current eps configuration.
2. Verify the <inst> parameter entry.
3. See the “[EPS Commands](#)” section on page [171](#).

Messages:

'instance' and 'enable|disable' required

Invalid number of peer's for this configuration

Invalid parameter error returned from MEP

MEP instance is not enabled

Meaning: You entered a MEP command but the command failed.

Recovery:

1. Review the particular command syntax and description.
2. Verify and re-enter the MEP command parameters.
3. See “[MEP Commands](#)” on page [175](#).

Messages:

Invalid parameter: 6660000

QCL Add failed: classified parameter missing

Meaning: You entered a QoS command but the command failed. For example:

```
QoS>port queueshaper rate 1 4 6660000
```

```
Invalid parameter: 6660000
```

Recovery:

1. Use the “show” version of the Aggregation commands
2. Verify the QoS command syntax.
3. See the “[QoS Commands](#)” on pages [187-209](#).

Message:

**Download of s3280fw from 192.168.1.30 failed: Operation timed out.
Error: Flash is already updated with this image**

Meaning: The firmware download failed or has already been updated to this version. For example:

```
>firmware load 192.168.1.30 s3280fw.dat
Download of s3280fw from 192.168.1.30 failed: Operation timed out.
>firmware load 192.168.1.30 S3280-v0.3.0.dat
Downloaded "S3280-v0.3.0.dat", 3561451 bytes
Error: Flash is already updated with this image
>
```

Recovery:

1. Enter the “firmware information” command to display information about the Active (current) and Alternate (available) firmware images.
2. Make sure the TFTP server is configured and running.
3. Verify the command syntax. See “[Firmware Commands](#)” on pages 212-214.
4. Check the TN web site for a more recent firmware version.

Message:

**east and west ports are same
failed in setting rpl block
given port is not configured either east or west for this group
given protection group does not exists
hold off should be configured in multiples of 100 ms - Invalid <hold_timeout> parameter: 1
incorrect error code = 36
incorrect error code = 37
incorrect error code = 4294967295
Invalid <group-id> parameter: 0
Invalid <rpl_port> parameter: 0
node is configured as neighbour for given group, can not set as rpl
this node is rpl owner for given protection group
vlans can not be deleted for this protection group**

Meaning: You entered an ERPS command but the command failed.

Recovery:

1. Review the particular command syntax and description.
2. Verify and re-enter the ERPS command parameters.
3. See “[ERPS Commands](#)” on pages 240-246.

Messages:

**E link_oam 22:53:06 61/eth_link_oam_mgmt_port_mib_retrival_oper_set#849: Error: Unable to retrieve the mode of the port(1/43)
E link_oam 23:02:10 61/eth_link_oam_mgmt_port_mib_retrival_oper_set#910: Error: Error:7 occurred while building MIB variable on port(1/0)
Requested configuration is already configured on port(1/1)**

Meaning: The “loam mib-retrival-support” command or “loam variable-retrieve” command failed.

Recovery:

1. Click the browser’s back button to clear the message, verify your selection, and then try the operation again.
2. Verify the requested configuration.
3. See “[LOAM Commands](#)” on pages 247-258.

Messages:

Invalid request on this port**Link OAM is not enabled on the port(1/1)****Requested configuration is not supported with the current OAM mode on port(1/1)****Requested operation is already in progress**

Meaning: You entered a LOAM command (e.g., loam variable-retrieve), but the command failed.

Recovery:

1. Review the particular LOAM command syntax and description.
2. Verify and re-enter the LOAM command parameters.
3. See "[LOAM Commands](#)" on pages 247-258.

Messages:

Deleting Protocol to Group mapping Failed**Invalid <mac_addr> parameter: 11:22:33:44:55:66**

Meaning: The attempted VCL command failed.

Recovery:

1. Review the specific VCL command syntax and description.
2. Verify the <mac_addr> parameter.
3. See "[VCL Commands](#)" on pages 276-279.

Message: **MVRP is not enabled Globally.**

Meaning: You entered a command to set or show the MVRP rrole ('restricted role') configuration, but did not first enable MVRP globally.

Recovery:

1. Enable MVRP globally before this command will function; use the **mvrp rrole enable** command.
2. Re-try the **mvrp control enable** command.
3. See "[MVRP Commands](#)" on pages 285-288.

Problem: **CPU can be overloaded by broadcast packets, causing loss of management.**

S3280 receiving excess broadcast packets causes loss of management.

Meaning: S3280 CPU overload and loss of management occur even when STP is discarding all packets from the port that the broadcasts are from, and when QoS Storm Control is configured to limit broadcast packets to rates as low as 1pps.

Recovery:

1. Enable Loop Protection.
2. See "[Loop Protection Configuration](#)".

Problem: Ingress Bandwidth profiling on Port doesn't allow for bursty TCP flows.

Meaning: The Port ingress policers work fine for traffic generation for normal L2 traffic streams. For TCP flow which is bursty in nature, the resultant bandwidth is very poor close to 10% of the set rate.

The issue can be that the leaky bucket for port ingress policer may not be set correctly to accommodate for the bursts mainly for TCP control frames.

Recovery:

1. Use EPL service which allows for bursty traffic flow.
2. See "[Ethernet Services](#)" on page 99.

Problem: MEP not working over link aggregation.

Meaning: Protocols above the LAG layer don't seem to consider the LAG group as a logical port (e.g., SOAM over an aggregated link). A MEP does not view the LAG group as a logical port; for example, if you:

1. Create an EVC with all LAG groups' ports in NNI.
2. Create a LAG group.
3. Create MEPs on the EVC (e.g., EVPL) service on UNI and NNI ports. Note that since a MEP has a residence port attached to it even though it's an EVC MEP, this creates issue when the residence port is down and CCMs are to be carried over the other ports. This creates faults on the MEP, possibly because of the MAC address being used in the CCMs.

Recovery: This is a deployment issue.

1. Use MEP on EVC instead; this is orthogonal to any aggregation. For a service running over an aggregation, just add all port to the NNI.

Problem: Management Port EtherType 9100 does not function

Meaning: When Management Port EtherType Customer S-port is set to 9100, S3280 access via Port 9 (MGMT port) is lost. This is a known issue with a fix in process, available at the next S3280 version release.

Recovery:

1. Make sure you are running the latest version of S3280 software; upgrade if a newer version is available.
2. If possible, use the S3280 CONSOLE PORT.
3. If possible, use EtherType 88A8 or 8100. See the "[Ports](#)" description on page 225.
4. Verify the APS and MEP configurations.
5. Retry the operation.

Problem: When ERPS is configured using a separate APS and SF MEPs, the S3280 will crash. The separate APS MEP is configured with CCM disabled and APS enabled.

Meaning: This is a known issue with a fix in process; available at the next S3280 version release.

The S3280 boot script runs, and a series of messages displays:

```
Warning: conf_sec_open failed or size mismatch, creating defaultsW erps 00:00:01 29/erps_init#1315:
Warning: conf_sec_open failed or size
mismatch, creating defaultsW link_oam 00:00:01 29/eth_link_oam_init#3012: Warning: conf_sec_open
failed or size mismatch, creating
defaultsPassword:
Login in progress...
Invalid username or password!
Username: adminPassword:
Login in progress...
Welcome to Transition Networks Command Line Interface (v1.0).
Type 'help' or '?' to get help.
```

Recovery:

1. Check the IP configuration. At the CLI prompt type **ip conf** and press **Enter**. For example:

```
>ip conf
IP Configuration:
=====
DHCP Client      : Enabled
IP Address       : 192.0.2.1
IP Mask          : 255.255.255.0
IP Router        : 0.0.0.0
VLAN ID          : 1
```

3. Make sure you are running the latest version of S3280 software; upgrade if a newer version is available.
4. Verify the APS and MEP configurations. See the related sections of this manual.
5. Retry the operation.

Message: fis load fails after firmware upgrade. The 'fis load -d managed' fails with one of the following errors after firmware upgrade:

decompression error: invalid block type
decompression error: invalid stored block lengths

Meaning: Flash Corruption and SPI Bus Access bug.

Recovery:

1. Boot managed.bk and run the firmware upgrade again.
2. When running the firmware upgrade again does not work, reprogramming the flash image has worked. Contact TN Support for direction.

Problem: Auto Negotiation between a 2.5G port and a 1G port does not work in S3280 v1.0.

Meaning: A check was added '&& (conf->speed == VTSS_SPEED_1G)', but 2.5G was missed. The S3280 software reads the SFP module and configures the link accordingly. On some systems it is not possible to read the SFP module via the I2C interface and this is the reason for the faulty behavior. This is a known issue with a fix in process; available at the next S3280 version release.

Recovery:

1. Make sure you are running the latest version of S3280 software; upgrade if a newer version is available.
2. Verify the port and auto-negotiation configurations. See the related sections of this manual.
3. Retry the operation.

Problem: Security level 11 appears to be equivalent to level 1

Meaning: When running at security level 11, only commands that work at levels 1 - 4 will display via the help, and do not seem to be otherwise available. This is a known issue with a fix in process, available at the next S3280 version release.

Recovery:

1. Do not use Security Level 11. Use Levels 10 and 12-14 instead.

Problem: Security level 1 help does not display correct results.

Meaning: Entering "S ?" in the CLI running under level 1 displays commands that do not work in level 1, and do not begin with the letter "s". The "System" command is available in limited form, but to get that information, "sy ?" must be entered. This is a known issue with a fix in process, available at the next S3280 version release.

Recovery: Use the "sy ?" command instead of the "S ?" command. For example:

1. Enter an "S ?" command which displays:

```
Command Groups:
-----
Switch : Switch security
Network : Network security
AAA : Authentication, Authorization and Accounting

Type '<group>' to enter command group
Type '<group> ?' to get group help
```

2. Enter an "sy ?" command which displays:

```
Available Commands:

System Configuration [all | (port <port_list>)]
System Log Configuration
System Version
System Log Lookup [<log_id>] [all|info|warning|error]
```

Problem: Errors displaying Sys Log Lookup command data.

Meaning: A series of cli_parser command errors display with the "sys log lookup" command. For example:

```
sys log lookup
Number of entries:
Info : 5
Warning: 0
Error : 176
All : 181
ID Level Time Message
-----
1 Info - Switch just made a cool boot.
2 Info 1970-01-01T00:00:02+00:00 Using primary power source.
3 Info 1970-01-01T00:00:09+00:00 Link up on port 1
4 Info 1970-01-04T02:51:12+00:00 Link down on port 1
5 Info 1970-01-04T02:51:46+00:00 Link up on port 1
6 Error 1970-01-07T00:08:56+00:00 E cli 97/cli_parse_command#2864: Er ...
7 Error 1970-01-07T00:08:56+00:00 E cli 97/cli_parse_command#2879: Er ...
8 Error 1970-01-07T00:08:56+00:00 E cli 97/cli_parse_command#2879: Er ...
9 Error 1970-01-07T00:08:56+00:00 E cli 97/cli_parse_command#2879: Er ...
```

Recovery:

1. Make sure you are running the latest version of S3280 software; upgrade if a newer version is available.
2. If possible, use the existing information as displayed.

Problem: the input **n ? ?** displays internal errors.

Meaning: Entering the command "**n > ?**" causes 'parse_command' internal error 2879 to display repeatedly.

For example:

```
test1:/>n ? ?
E cli 139/cli_parse_command#2864: Error: Internal error
E cli 139/cli_parse_command#2879: Error: Internal error
E cli 139/cli_parse_command#2879: Error: Internal error
E cli 139/cli_parse_command#2879: Error: Internal error
E cli 139/cli_parse_command#2879: Error: Internal error
E cli 139/cli_parse_command#2879: Error: Internal error
E cli 139/cli_parse_command#2879: Error: Internal error
E cli 139/cli_parse_command#2879: Error: Internal error
E cli 139/cli_parse_command#2879: Error: Internal error
E cli 139/cli_parse_command#2879: Error: Internal error
E cli 139/cli_parse_command#2879: Error: Internal error
E cli 139/cli_parse_command#2879: Error: Internal error
E cli 139/cli_parse_command#2879: Error: Internal error
E cli 139/cli_parse_command#2879: Error: Internal error
E cli 139/cli_parse_command#2879: Error: Internal error
E cli 139/cli_parse_command#2879: Error: Internal error
E cli 139/cli_parse_command#2879: Error: Internal error
```

Recovery:

1. Make sure you are running the latest version of S3280 software; upgrade if a newer version is available.
2. If possible, use the existing information displayed, or try using another CLI command.

Problem: Can no longer HTTPS browse to S3280 after new certificate is generated.

Meaning: Initially enabling HTTPS and browsing to the S3280 with HTTPS works. However, if a new certificate is generated, any web browser that previously navigated the S3280 via https (using the old certificate) can no longer HTTPS browse the S3280. This may be because when a new certificate is generated, it re-uses the original certificate's serial number. This is a known issue with a fix in process, available at the next S3280 version release.

Recovery:

1. Make sure you are running the latest version of S3280 software; upgrade if a newer version is available.
2. If possible, use the existing certificate.

Message:

eth: DAD detected duplicate IPv6 address ::c000:0201: NS in/out=0/3, NA in=1
eth: DAD complete for ::c000:0201 - duplicate found
eth: manual intervention required
possible hardware address duplication detected, disable IPv6

Meaning: A possible hardware address duplication was detected.

During the stateless autoconfiguration process, duplicate address detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection is performed first on the new link-local address. When the link local address is verified as unique, then duplicate address detection is performed on all other IPv6 unicast addresses on the interface.

Duplicate address detection is suspended on interfaces that are administratively down. While an interface is administratively down, the unicast IPv6 addresses assigned to the interface are set to a 'pending' state. An interface returning to an administratively up state restarts duplicate address detection for all of the unicast IPv6 addresses on the interface.

When a duplicate address is identified, the state of the address is set to 'Duplicate', the address is not used, and the above error message displays.

If the duplicate address is a global address, the address is not used. Recovery is automatically performed.

If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface.

Recovery:

1. Provide a valid, unique IPv6 address for this S3280.
2. Enter the **ip config** command to verify the current IP configuration settings.
3. Disable IPv6 temporarily, retry the operation, and then enable IPv6 again.
4. Disable IPv6 Auto Configuration temporarily, retry the operation, and then enable IPv6 again.
5. When successful, the new message "**DAD complete for ::c000:0201 -9 - no duplicates found**" displays.

Message:

Backup Error
HTTPS Certificate Generate Error
Restore Error

Meaning: A problem was detected in the privilege level checks for TN web pages.

Recovery:

1. Check the user privilege level to make sure the current level assigned has access to the attempted function.
2. Either try another command or have the user privilege level changed to a higher level.
3. Contact TN support if the problem persists.

Messages:

W mvr 20:55:15 10/mvr_stacking_set_intf_entry#1685: Warning: MVR delete VLAN-1 failed in isid-1

W mvr 22:01:59 46/_mvr_vlan_warning_handler#4112: Warning: Please adjust the management VLAN ports overlapped with MVR source ports!

Meaning: An error occurred in the MVR configuration.

Recovery:

1. Note the specific message.
2. Re-configure the MVR or VLAN port configuration. See the related section of this manual.

Message: >E api 00:28:25 57/vtss_vcap_add#640: Error: VCAP ISI: Could not find ID: 2
E web 00:28:25 57/handler_config_evc_edit#311: Error: evc_mgmt_add(0): failed

Meaning: At the S3280 **Configuration > Ethernet Services** menu path, you tried to set up the ECE before setting up the related EVC.

At the CLI, you entered one of the EVC ECE commands before entering the related EVC commands.

Recovery: Set up the EVC before trying to set up the ECE.

Message: **1 Error 1970-01-01T00:00:00+00:00 E misc 00:00:00 26/hpic_spi_init_st ...**

Meaning: An internal incompatibility exists.

Recovery:

1. Check the current firmware version and upgrade as necessary.
2. Reboot your computer.
3. Contact TN Support.

Message: **arp: 00-c0-f2-21-b8-c4 is using my IP address 192.168.1.110!**

Meaning: An IP address conflict exists.

Example 1:

```
>ip setup 192.168.1.110 255.255.255.0 192.168.1.1
>arp: 00-c0-f2-21-b8-c4 is using my IP address 192.168.1.110!
```

Example 2:

```
>config backup bin 192.168.1.30 v1.1.1bucfg
arp: 00-c0-f2-21-b8-c4 is using my IP address 192.168.1.110!
arp: 00-c0-f2-21-b8-c4 is using my IP address 192.168.1.110!
arp: 00-c0-f2-21-b8-c4 is using my IP address 192.168.1.110!
arp: 00-c0-f2-21-b8-c4 is using my IP address 192.168.1.110!
arp: 00-c0-f2-21-b8-c4 is using my IP address 192.168.1.110!
tftp client put failed: 8
>
```

Recovery:

1. Check the current **'ip config'** parameters and change as necessary.
2. Reboot your computer.
3. Contact TN Support.

Message: **W mvr 02:25:04 48/_mvr_vlan_warning_handler#4230: Warning: Please adjust the management VLAN ports overlapped with MVR source ports!**

Meaning: At **Configuration > MVR > VLAN Interface Setting** you set a Port Role to S:Source or R:Receiver, and that setting is in conflict with a Management VLAN port setting.

Recovery:

1. Cycle power.
2. Log in again via CLI.
- 3a. CLI: enter the **config default keep** command and press **Enter**.
- 3b. Web interface: at **Maintenance > Factory Defaults** select **Yes**.

Problem: When the FDB table reaches 8192 entries, a new dynamic MAC will be learned and override the old one.

Description: When the MAC table is full (8192 entries), the switch learns new entries and purges older entries even though these entries are not aged. This is the expected behavior. The MAC table is implemented so that it will always store the most active entries. The least recently used entries are removed to provide storage for new entries. The benefit of this approach is that in a normal network, flooding is kept to a minimum when the MAC table becomes full. This occurs even when aging is disabled. This behavior is not configurable.

Resolution:

1. Apply Port- or MAC-based authentication (IEEE802.1X).
2. Set up a per-port MAC table limit, preventing an intruder from taking up too much of the MAC table. For example, if a port is limited to 64 entries in the MAC table, frames causing this limit to be exceeded are discarded, and the MAC table is not affected.
3. Set up additional Storm Policers to prevent flooding on an unknown MAC address. See the **Configuration > QoS** section.

Problem: The "psec_limit" cannot work when configuration "limit" is "1024".

The S3280 fails to send the trap only when the limit control reaches '1024' at the 5 packets/sec. rate.

Also, some the highwarn and normal DMI traps occur when the limit parameter reaches '1023' or '1024'.

Description: This is a Port Security Limit Control issue where the software is unable to process the new Mac address frames in time. It is receiving frames faster than it can add to the Mac table and in turn looks like it is losing frames, thus not reaching the limit. In a normal scenario if new Mac addresses turns up for example, once a second, it will work. But in case of an attack of new Mac address, then the port won't shutdown, but it won't switch these frames either. The S3280 works fine when tested at 5 frames/second.

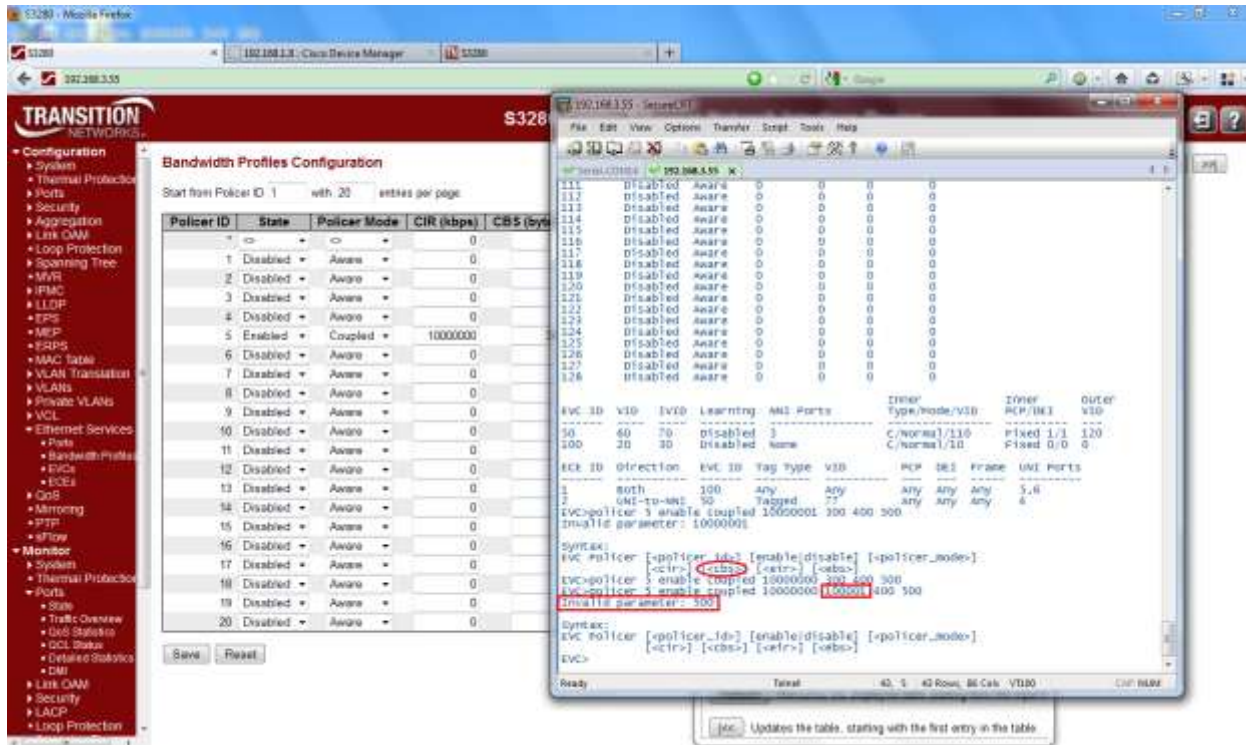
Resolution:

1. Decrease the limit to less than 200 (the security network limit limit 194).
2. Check for upgrades with a fix to this known problem.

Message / Problem: “Invalid parameter” message displays when a valid parameter entered

Meaning: This is not an error. This is the intended way the parser works by design. If you set CBS value to 100001, you would expect that since this is an invalid value, a warning should display that the 100001 entry is invalid, but it displays the wrong information that the EBS value is invalid.

Example:



The command syntax is: **EVC Policer** [<policer_id>] [enable|disable] [<policer_mode>] [<cir>] [<cbs>] [<eir>] [<ebs>]

When entered as **EVC Policer 1 enable aware 4 100001 1 1**

1. 4 is tried as cir and succeeds.
2. 100001 is tried as cbs but fails.
3. cbs is optional so 100001 is tried as eir and succeeds.
4. 1 is tried as ebs and succeeds.
5. There are no parameters left to match, so the remaining 1 returns an error.

If you enter the command without the last parameter 1, it will succeed and you can see which parameters were filled:

```

>EVC Policer 1 enable aware 4 100001 1
>EVC Policer 1
Policer State      Mode      CIR      CBS      EIR      EBS
-----
1         Enabled   Aware    4         0         100001   1
>
    
```

Message: E web 00:10:06 60/httpd_form_get_value_int#799: Error: Unknown form. Form name = thermal_port_prio_12, form_value = 12

Meaning: A discrepancy exists in the thermal port or thermal priority configuration.

Recovery:

1. Verify the “thermal” command parameters.

Problem: 'System Restore Default' hangs intermittently and indefinitely.

Meaning: This appears to only happen when an EVC/ECE is configured. In S3280 v1.2.1 and above, EVC and ECE configurations are removed when you execute a System Restore via the web (Maintenance > Configuration > Restore Binary) or via the CLI (config restore binary command).

Recovery:

1. If the EVC/ECE is removed before defaulting then the command will not hang.
2. Upgrade the S3280 to the latest software version.

Message:

E snmp 22:02:10 8/snmpDMINotification#442: Error: Notification for dmi failed due to insufficient memory.

E snmp 22:02:11 8/trap_bind_var#172: Error: FATAL: cannot malloc in trap_bind_var

Meaning: An S3280 memory error condition exists.

Recovery:

1. Re-configure the recent configuration changes.
2. Upgrade the S3280 to the latest software version.

Message:

W conf 02:44:14 60/conf_tn_bin_restore#1076: Warning: config buffer is invalid

W web 02:44:14 60/handler_config_restore_binary#405: Warning: Restore from binary config failed

Meaning: A failure occurred during a Restore procedure.

Recovery:

1. Verify the restore file name and size, and re-try the operation.
2. See the “**Error! Reference source not found.**” on page **Error! Bookmark not defined.**
3. Upgrade the S3280 to the latest software version.

Message:

W mvr 01:41:59 48/_mvr_vlan_warning_handler#4230: Warning: Please adjust the management VLAN ports overlapped with MVR source ports!

W mvr 03:10:22 60/mvr_stacking_set_intf_entry#1937: Warning: MVR delete VLAN-1 failed in isid-1

Meaning: You assigned the same port to the Management VLAN and the MVR ‘Immediate Leave Setting’.

Recovery:

1. Either change the MVR configuration, or change the Management VLAN port assignment.
2. Delete any entries in the VLAN Interface Setting table.
3. Retry the operation.

Message: Loopback VLAN %d not found

Meaning: The VLAN ID (VID) for the EtherSAT Loopback was not found.

Recovery:

1. Verify the parameters entered and re-try the EtherSAT loopback test.
2. See “[EtherSAT Loopback Configuration Commands \(S3280-TST Only\)](#)” on page 355.

Message:

Max tries exceeded while waiting for loopback to become inactive

Max tries exceeded while waiting for loopback to become active

Meaning: A timeout occurred before the loopback became active / inactive.

Recovery:

1. Verify the parameters entered and re-try the EtherSAT loopback test.
2. See “[EtherSAT Loopback Configuration Commands \(S3280-TST Only\)](#)” on page 355.

Message:

TX and RX path is disabled

Unable to reset Altera MC Control

Unable to reset Altera PCS Control

Meaning: An internal S3280-TST EtherSAT problem occurred.

Recovery:

1. Verify the parameters entered and re-try the EtherSAT loopback test.
2. See “[EtherSAT Loopback Configuration Commands \(S3280-TST Only\)](#)” on page 355.

Message:

E api/cil 00:20:30 28/126_action_check#5522: Error: ACL policer and EVC policer can not both be enabled

Meaning: You have enabled ACL policer and EVC policer concurrently, which is not a valid configuration.

Recovery:

1. Disable either the ACL policers or the EVC policers.
2. See the “Set / Show ACL Port Default Action” command or the “EVC Policer” command.
3. Retry the operation.

Message:

Peer MAC address should be unicast

Peer MAC is needed for HW based CCM.

Peer MAC is needed for CCM rates 300f/sec and 100f/sec

Peer MAC should be non-zero for HW Generated CCM

Peer MAC should be unicast.

Meaning: The "Unicast Peer MAC" option only supports the unicast address to be configured.

Recovery:

1. Change the MEP configuration. See the “mep peer mep” command.
2. Retry the operation.

Message: Setting Tx mirroring for mirror port (port %lu) has no effect. Tx mirroring ignored.

Meaning: If you set an invalid value to the Mirroring Mode, this SNMP error displays.

Recovery:

1. Select a valid Mirror Mode entry (e.g., enable, disable, rx, or tx).
2. See the “Mirror Configuration”, “Mirror Port”, or “Mirror Mode” command.

Message:

syslog Clear Level = %ld

syslog message get info fail!
syslog server address to set is: %s
Testing syslog number %d (prefix: Debug, Info, Warning, etc.)

Meaning: You entered an invalid Syslog entry.

Recovery:

1. Select a valid Syslog entry.
2. See the “System Log Server Address”, “System Log Configuration”, or “System Log Level” command.

Message:

txt2ipv4 failed for tnIpAddr = %s (IP Mgmt Table Entry)
txt2ipv4 failed for tnSubnetMask = %s(IP Mgmt Table Entry)
Configuration failed (DefaultGateway table entry)

Meaning: An error occurred when configuring the DNS Server.

Recovery:

1. Select a valid DNS entry.
2. See the “IP DNS” or “IP DNS Proxy” command.

Message:

acl_mgmt_ace_add failed
mac_mgmt_learn_mode_set failed: %d
vtss_esce_add failed

Meaning: On the S3280-TST, the FPGA port has learning disabled.

Recovery:

1. Select another S3280-TST port and continue operation.

Message:

Error: Part of the VLAN configuration didn't apply as some of ports are in forbidden list for a given VLAN id.
Error: Part of the VLAN configuration didn't apply as some of ports are in member list for a given VLAN id.
notice: forbidden port cannot overlap with egress member port in MIB setting.

Meaning: The system does not allow changing VLAN member ports once there is forbidden port (or ports) in this VLAN.

Recovery:

1. Change either the VLAN member ports configuration or change the VLAN forbidden ports configuration.
2. See the “VLAN add” command or “VLAN forbidden” command in this manual.

Message:

ACL rate limiter and EVC policer can not both be enabled
Error: ACL policer and EVC policer can not both be enabled
'Rate Limiter' and 'EVC Policier' can not both be enabled

Meaning:: CLI will pop up message after enable ACL policer and EVC policer on ACL_Ports by WEB/SNMP

Recovery: S3280-xxx hardware can not support both ACL policer and EVC policer enabled in an ACE entry.

This Web/CLI/SNMP check rule is implemented to avoid this invalid parameter entry.

1. Disable either the ACL policer or the EVC policer on ACL ports via the Web GUI or SNMP.
2. Continue operation.
3. See the related section of the related manual.

Message: Unable to Run

PTP clock is not created on Initiator.

Meaning: This is a PTP validation error. If PTP is not created and RFC2544 latency is chosen and you run the test, this error displays and the RFC2544 latency test will not run.

Recovery:

1. Configure a PTP clock instance to ensure accurate RFC 2544 Latency test step timestamps.
2. Make sure PTP is running on both devices to synchronize the Time of Day. See “[PTP Commands](#)” on page 271.
3. Retry the operation. See the *RFC 2544 User Guide* for more RFC2544 latency test information.

System Log Messages

The S3280 displays four levels of syslog messages as explained below. Note that the **All** level displays all three levels of information that the S3280 can logged (Info, Warning, and Error).

```
>system log lookup
Number of entries:
Info      : 7
Warning: 0
Error    : 5
All      : 12
```

ID	Level	Time	Message
1	Info	-	Switch just made a cool boot.
2	Info	1970-01-01T00:00:02+00:00	Link up on port 6
3	Info	1970-01-01T00:00:02+00:00	Using primary power source.
4	Info	1970-01-01T00:00:07+00:00	Link up on port 3
5	Error	1970-01-01T00:26:54+00:00	VLAN Port Configuration Ingress Fil ...
6	Error	1970-01-01T00:26:54+00:00	VLAN Port Configuration Ingress Fil ...
7	Error	1970-01-01T00:26:54+00:00	VLAN Port Configuration Ingress Fil ...
8	Error	1970-01-01T00:26:54+00:00	VLAN Port Configuration Ingress Fil ...
9	Info	1970-01-01T03:31:43+00:00	Link down on port 6
10	Info	1970-01-04T01:15:48+00:00	Link down on port 3
11	Info	1970-01-04T01:15:54+00:00	Link up on port 3
12	Error	1970-01-04T01:15:54+00:00	VLAN Port Configuration Ingress Fil ...

```
>
```

Info Level Messages

These are the Information level messages of the system log. These are normal operational messages used for reporting, measuring throughput, etc. This level of message requires no action.

Table 3. Syslog Info Messages

Info Level Message	Description
<i>Switch just made a cold boot.</i>	The S3280 was restarted. See " Maintenance > Restart Device ". No action required.
<i>Link up on port x</i>	The most recent link status on the port x is 'link up'. Port Link is up - no action needed.
<i>Link down on port x</i>	The most recent link status on the port x is 'link down'. See Configuration > Ports > Port Configuration . No action required.
<i>Using primary power source.</i>	Normal power on operation. No action required.
<i>Frame of 243 bytes received on port 1MAC</i>	Normal frame size information. No action required.
<i>Port 1 shut down</i>	Normal port shutdown information. No action required.

Warning Level Messages

These messages are the Warning level of the system log. These Warning messages are not an error, but an indication that an error will occur if action is not taken (e.g. file system 85% full). Each item must be resolved within a given time.

Table 4. Syslog Warning Messages

Warning Level Message	Description
<i>E api/cil 17:42:26 29/126_action_check#6036:</i>	ACL policer and EVC policer can not both be enabled. Disable one or the other.

Error Level Messages

Error level messages of the system log. These non-urgent failures should be relayed to a developer or an administrator.

Each item must be resolved within a given time.

Table 5. Syslog Error Messages

Error Level Message	Description
<i>E api/cil 17:42:45 29/126_acl_policer_free#6069:</i>	Error: policer 0 already free. The EVC policer or ACL policer. See the related section of this manual.
<i>VLAN Port Configuration Ingress Filter Conflict - MSTP</i>	Verify the Ingress Policers, Port Policing, or Queue Policing configuration. See the Configuration > Security > Network > ACL or the Configuration > QoS menu path.
<i>VLAN Port Configuration Ingress Filter Conflict - ERPS</i>	Verify the ERPS, VLAN, and port configurations. See the related section of this manual.

Note that the **All** level displays all three levels of information that the S3280 can logged (Info, Warning, and Error).

Third Party Program Messages

The S3280 displays error and information messages from various third party applications, such as Internet Explorer, HyperTerminal, PuTTY, etc. This section lists the messages, provides an example, and discusses the message meaning of and possible recovery steps.

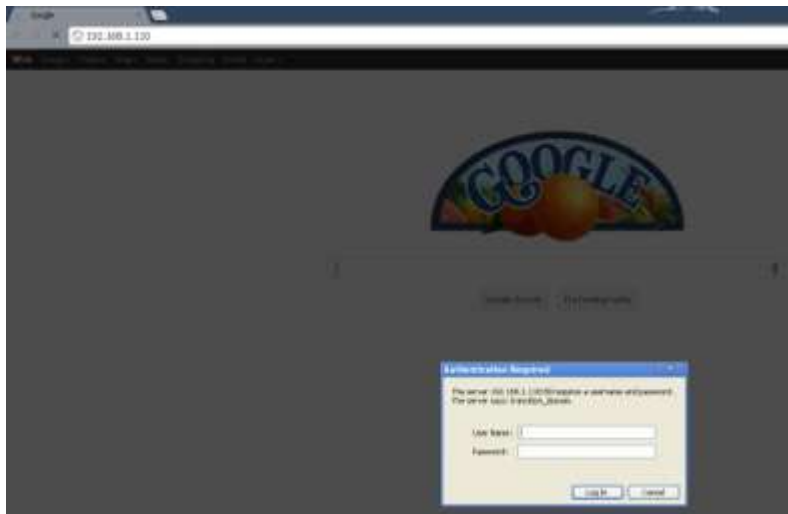
Message: PuTTY Security Alert - The server's host key is not cached in the registry.



Meaning: Normal PuTTY login security message.

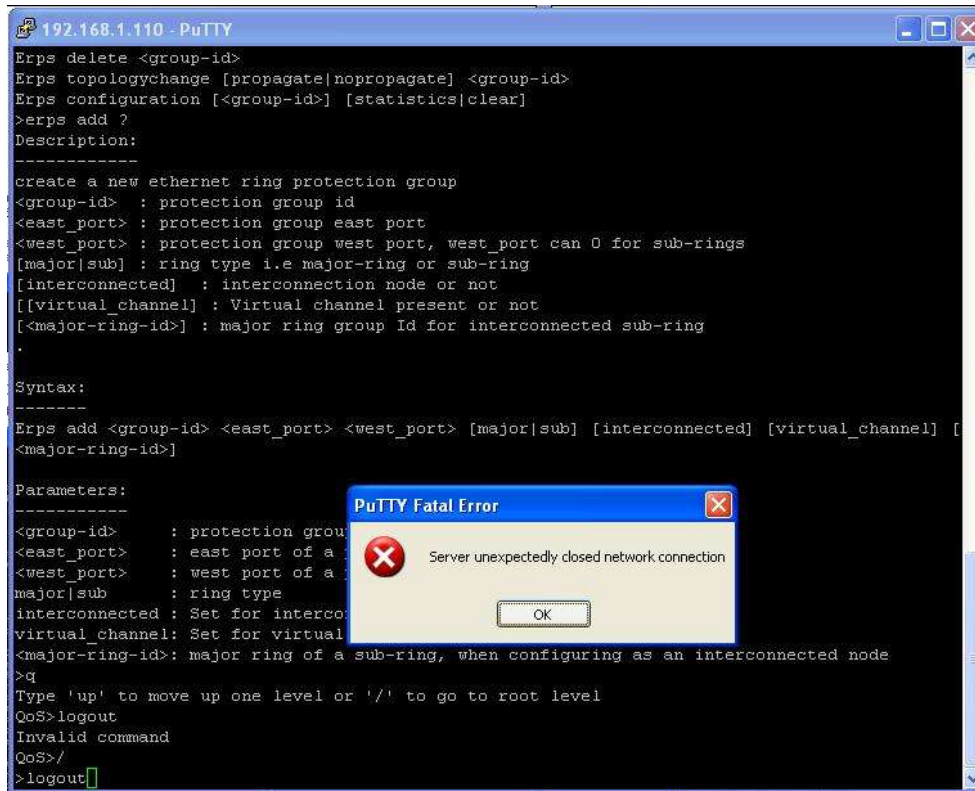
Recovery: Click the **Yes** button to trust this host, add the key to the PuTTY cache, and clear the message.

Message: Authentication Required



Meaning: Normal Google Chrome login screen.

Recovery: Enter your S3280 User Name and Password, and click the **Log In** button.

Message: PuTTY Fatal Error - Server unexpectedly closed network connection


```

192.168.1.110 - PuTTY
Erps delete <group-id>
Erps topologychange [propagate|nopropagate] <group-id>
Erps configuration [<group-id>] [statistics|clear]
>erps add ?
Description:
-----
create a new ethernet ring protection group
<group-id> : protection group id
<east_port> : protection group east port
<west_port> : protection group west port, west_port can 0 for sub-rings
[major|sub] : ring type i.e major-ring or sub-ring
[interconnected] : interconnection node or not
[[virtual_channel] : Virtual channel present or not
[<major-ring-id>] : major ring group id for interconnected sub-ring
.

Syntax:
-----
Erps add <group-id> <east_port> <west_port> [major|sub] [interconnected] [virtual_channel] [
<major-ring-id>]

Parameters:
-----
<group-id> : protection group id
<east_port> : east port of a protection group
<west_port> : west port of a protection group
major|sub : ring type
interconnected : Set for interconnected node or not
virtual_channel : Set for virtual channel
<major-ring-id> : major ring of a sub-ring, when configuring as an interconnected node
>q
Type 'up' to move up one level or '/' to go to root level
QoS>logout
Invalid command
QoS>/
>logout
  
```

Meaning: The PuTTY application suffered a fatal internal error.

Recovery:

1. Click the **OK** button to close the message dialog box.
2. Close the PuTTY session window.
3. Start a new PuTTY session.

Message: Unknown parameter: [<dmirxpwrinthr>]

Example:

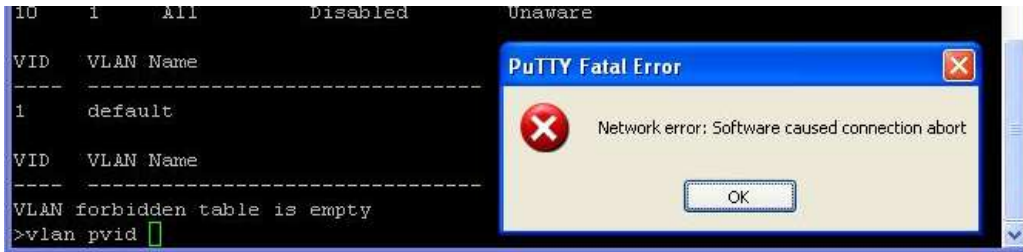
```

>port dmi
Unknown parameter: [<dmirxpwrinthr>]
>
  
```

Meaning: The parameter you entered was not recognized.

Recovery:

1. See the related command section for specific information.
2. Make sure the S3280 firmware is the latest and upgrade if a newer version is available.

Message: PuTTY Fatal Error - Network Error: Software caused connection abort

Meaning:

Recovery:

1. Click the **OK** button to clear the PuTTY message.
2. Exit the PuTTY screen.
3. Start a new PuTTY session and log in to the S3280.
4. Verify the command entered and retry the operation.
5. If the problem persists, contact TN Tech Support.

Message: File <S3280-master> : error 2 in system call CreateFile The system cannot find the file specified.
[10/08 13:32:19.959]

Meaning: The TFTP Server cannot find the file that you specified for downloading.

Recovery:

1. Make sure the TFTP Server "Current Directory" points to C:\TFTP-Root.
2. Make sure that you have specified the correct file (xxxxxxx.DAT).
3. See "[Firmware Commands](#)" on page 261.

Recording Model and System Information

After performing the troubleshooting procedures, and before calling or emailing Technical Support, please record as much information as possible in order to help the TN Technical Support Specialist.

1. From the CLI, use the commands needed to gather the information requested below (e.g., **system config**, **system log config**, **system version**, **ip config**, or others as request by the TN Tech Support Specialist.)

From the S3280 web interface, select the **Monitor > System > Information** menu path.

2. Record the **model information** for your S3280.

Product ID _____ MAC Address _____

Serial # _____ Chip ID _____

System Date _____ System Uptime _____

Software Version _____ Software Date _____

FPGA Version: _____ Operating System: _____

Browser: _____

3. Provide additional Model and System information to your Technical Support Specialist. See “Basic Troubleshooting” in the *S3280 User Guide, 33506*.

Your Transition Networks service contract number: _____

Describe the failure: _____

Describe any action(s) already taken to resolve the problem (e.g., rebooting, troubleshooting steps, etc.):

The serial and revision numbers of all involved Transition Networks products in the network:

Describe your network environment (layout, cable type, etc.): _____

Network load and frame size at the time of trouble (if known): _____

The device history (i.e., have you returned the device before, is this a recurring problem, etc.):

Any previous Return Material Authorization (RMA) numbers: _____

Technical Support

Technical support is available 24-hours a day at:

United States: 1-800-260-1312
International: 00-1-952-941-7600

Live Web chat

Chat live via the Web with a Transition Networks Technical Support Specialist.

Go to: <http://www.transition.com/TransitionNetworks/Now.aspx>

Click [Transition NOW](#) to begin a live chat session.

Web-based training

Transition Networks provides 12-16 seminars per month via live web-based training.

Log onto www.transition.com and click the [Learning Center](#) link at the top of the page.

E-Mail

Ask a question anytime by sending an e-mail message to our technical support staff: techsupport@transition.com.

Address

Transition Networks
10900 Red Circle Drive
Minnetonka, MN 55343, U.S.A.
Telephone: 952-941-7600
Toll free U.S.A & Canada: 800-526-9267
Fax: 952-941-2322

S3280 CLI Command Summary by Group

The S3280 has 32 command groups and approximately 500 commands. Note that the item numbers below are added for reference purposes only.

Command Groups

>**help**

General Commands:

Help/? : Get help on a group or a specific command

Up : Move one command level up

Logout: Exit CLI

Command Groups:

```
System      : System settings and reset options
Conf        : Configuration management
Loop        : Loop Protection
IP          : IP configuration and Ping
Port        : Port management
MAC         : MAC address table
VLAN        : Virtual LAN
PVLAN       : Private VLAN
Security    : Security management
STP         : Spanning Tree Protocol
Aggr        : Link Aggregation
LACP        : Link Aggregation Control Protocol
LLDP        : Link Layer Discovery Protocol
Thermal     : Thermal Protection
EVC         : Ethernet Virtual Connections
EPS         : Ethernet Protection Switching
MEP         : Maintenance entity End Point
QoS         : Quality of Service
Mirror      : Port mirroring
Firmware    : Download of firmware via TFTP
PTP         : IEEE1588 Precision Time Protocol
MVR         : Multicast VLAN Registration
ERPS        : Ethernet Ring Protection Switching
LOAM        : Ethernet Link OAM
Loop Protect: Loop Protection
IPMC        : MLD/IGMP Snooping
sFlow       : sFlow Agent
VCL         : VLAN Control List
EtherSAT    : Ethernet Service Activation Testing
SIR         : Static IP Routing
```

Type '<group>' to enter command group, e.g. 'port'.

Type '<group> ?' to get list of group commands, e.g. 'port ?'.

Type '<command> ?' to get help on a command, e.g. 'port mode ?'.

Commands may be abbreviated, e.g. 'por co' instead of 'port configuration'.

>

Note: The S32880-TST models have **EtherSAT** commands and **Firmware Peripheral** commands that the S3280 does not support.

General Commands

1. Help/?: Get help on a group or a specific command
2. Up : Move one command level up
3. Logout: Exit CLI

System Commands

4. System Configuration [all | (port <port_list>)]
5. System Log Configuration
6. System Timezone Configuration
7. System Version
8. System Log Server Mode [enable|disable]
9. System Name [<name>]
10. System Timezone Offset [<offset>]
11. System Contact [<contact>]
12. System Log Server Address [<ip_addr_string>]
13. System Timezone Acronym [<acronym>]
14. System DST Configuration
15. System Location [<location>]
16. System Log Level [info|warning|error]
17. System DST Mode [disable|recurring|non-recurring]
18. System DST start <week> <day> <month> <date> <year> <hour> <minute>
19. System Log Lookup [<log_id>] [all|info|warning|error]
20. System DST end <week> <day> <month> <date> <year> <hour> <minute>
21. System Log Clear [all|info|warning|error]
22. System Reboot
23. System Date
24. System DST Offset [<dst_offset>]
25. System PowerSupply Active
26. System Load

Config Commands

27. Config Backup Binary <hostname> <file_name>
28. Config Restore Binary <hostname> <file_name>
29. Config Default [keep_ip]

Loop Protect Commands

30. Loop Protect Configuration
31. Loop Protect Mode [enable|disable]
32. Loop Protect Transmit [<transmit-time>]
33. Loop Protect Shutdown [<shutdown-time>]
34. Loop Protect Port Configuration [<port_list>]
35. Loop Protect Port Mode [<port_list>] [enable|disable]
36. loop protect port action [<port_list>] [shutdown|trap|log|shut_log|shut_trap|log_trap|all]
37. Loop Protect Port Transmit [<port_list>] [enable|disable]
38. Loop Protect Status [<port_list>]

IP Commands

39. IP ARP Show
40. IP Configuration
41. IP DHCP [enable|disable]
42. IP Setup [<ip_addr>] [<ip_mask>] [<ip_router>]
43. IP Ping <ip_addr_string> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)]
44. IP DNS [<ip_addr>]
45. IP DNS_Proxy [enable|disable]

46. IP IPv6 AUTOCONFIG [enable|disable]
47. IP IPv6 Setup [<ipv6_addr>] [<ipv6_prefix>] [<ipv6_router>]
48. IP IPv6 State <ipv6_addr> [enable|disable]
49. IP IPv6 Ping6 <ipv6_addr> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)]
50. IP MVLan [<vid>]
51. IP NTP Configuration
52. IP NTP Mode [enable|disable]
53. IP NTP Server Add <server_index> <ip_addr_string>
54. IP NTP Server Ipv6 Add <server_index> <server_ipv6>
55. IP NTP Server Delete <server_index>

Port Commands

56. Port Configuration [<port_list>] [up|down]
57. Port Mode [<port_list>] [auto|10hdx|10fdx|100hdx|100fdx|1000fdx|sfp_auto_ams]
58. Port Flow Control [<port_list>] [enable|disable]
59. Port State [<port_list>] [enable|disable]
60. Port MaxFrame [<port_list>] [<max_frame>]
61. Port Power [<port_list>] [enable|disable|actiphys|dynamic]
62. Port Excessive [<port_list>] [discard|restart]
63. Port Statistics [<port_list>] [<command>] [up|down]
64. Port VeriPHY [<port_list>]
65. Port SFP [<port_list>]
66. Port DMI Configuration [<port_list>] [<dmi_rx_pwr_int_thr>]
67. Port DMI Statistics [<port_list>]
68. Port Description [<port_list>] [<name>]

MAC Commands

69. MAC Configuration [<port_list>]
70. MAC Add <mac_addr> <port_list> [<vid>]
71. MAC Delete <mac_addr> [<vid>]
72. MAC Lookup <mac_addr> [<vid>]
73. MAC Agetime [<age_time>]
74. MAC Learning [<port_list>] [auto|disable|secure]
75. MAC Dump [<mac_max>] [<mac_addr>] [<vid>]
76. MAC Statistics [<port_list>]
77. MAC Flush

VLAN Commands

78. VLAN Configuration [<port_list>]
79. VLAN Translation Add <group_id> <vid> <trans_vid>
80. VLAN PVID [<port_list>] [<vid>|none]
81. VLAN Translation Delete <group_id> <vid>
82. VLAN FrameType [<port_list>] [all|tagged|untagged]
83. VLAN Translation Group [<port_list>] [<group_id>]
84. VLAN IngressFilter [<port_list>] [enable|disable]
85. VLAN tx_tag [<port_list>] [untag_pvid|untag_all|tag_all]
86. VLAN PortType [<port_list>] [unaware|c-port|s-port|s-custom-port]
87. VLAN MPort PortType [unaware|c-port|s-port|s-custom-port]
88. VLAN remove <vid>|<name> [<port_list>]
89. VLAN EtypeCustomSport [<etype>]
90. VLAN Add <vid>|<name> [<ports_list>]
91. VLAN Forbidden Add <vid>|<name> [<port_list>]
92. VLAN Delete <vid>|<name>
93. VLAN Forbidden Delete <vid>|<name>
94. VLAN Forbidden Lookup [<vid>] [(name <name>)]
95. VLAN Lookup [<vid>] [(name <name>)] [combined|static|nas|mvr|evc|all]

- 96. VLAN Name Add <name> <vid>
- 97. VLAN Name Delete <name>
- 98. VLAN Name Lookup [<name>]
- 99. VLAN Status [<port_list>] [combined|static|nas|mvr|mstp|erps|mep|vcl|all|conflicts]

PVLAN Commands

- 100. PVLAN Configuration [<port_list>]
- 101. PVLAN Add <pvlan_id> [<port_list>]
- 102. PVLAN Delete <pvlan_id>
- 103. PVLAN Lookup [<pvlan_id>]
- 104. PVLAN Isolate [<port_list>] [enable|disable]

Security Commands

Switch : Switch security command groups

Security Switch Users : User management

- 94. Security Switch Users Configuration
- 95. Security Switch Users Add <user_name> <password> <privilege_level>
- 96. Security Switch Users Delete <user_name>

Security Switch Privilege: Privilege level

- 97. Security Switch Privilege Level Configuration
- 98. Security Switch Privilege Level Group <group_name> [<cro>] [<crw>] [<sro>] [<srw>]
- 99. Security Switch Privilege Level Current

Security Switch Auth : Authentication

- 101. Security Switch Auth Configuration
- 102. Security Switch Auth Method [console|telnet|ssh|web] [none|local|radius|tacacs+] [enable|disable]

Security Switch SSH : Secure Shell

- 103. Security Switch SSH Configuration
- 104. Security Switch SSH Mode [enable|disable]

Security Switch HTTPS : Hypertext Transfer Protocol over Secure Socket Layer

- 105. Security Switch HTTPS Configuration
- 106. Security Switch HTTPS Mode [enable|disable]
- 107. Security Switch HTTPS Redirect [enable|disable]
- 108. Security Switch HTTPS Certificate Show
- 109. Security Switch HTTPS Certificate Generate [rsa|dsa]
- 110. Security Switch HTTPS Certificate Load <hostname> <file_name>

Security Switch Access : Access management

- 111. Security Switch Access Configuration
- 112. Security Switch Access Mode [enable|disable]
- 113. Security Switch Access Add <access_id> <start_ip_addr> <end_ip_addr> [web] [snmp] [telnet]
- 114. Security Switch Access Ipv6 Add <access_id> <start_ipv6_addr> <end_ipv6_addr> [web] [snmp] [telnet]
- 115. Security Switch Access Delete <access_id>
- 116. Security Switch Access Lookup [<access_id>]
- 117. Security Switch Access Clear
- 118. Security Switch Access Statistics [clear]

Security Switch SNMP : Simple Network Management Protocol

- 119. Security Switch SNMP Configuration
- 120. Security Switch SNMP Mode [enable|disable]
- 121. Security Switch SNMP Version [1|2c|3]
- 122. Security Switch SNMP Read Community [<community>]
- 123. Security Switch SNMP Write Community [<community>]
- 124. Security Switch SNMP Trap Mode [enable|disable]
- 125. Security Switch SNMP Trap Version [1|2c|3]
- 126. Security Switch SNMP Trap Community [<community>]
- 127. Security Switch SNMP Trap Destination [<ip_addr_string>]

128. Security Switch SNMP Trap IPv6 Destination [<ipv6_addr>]
129. Security Switch SNMP Trap Authentication Failure [enable|disable]
130. Security Switch SNMP Trap Link-up [enable|disable]
131. Security Switch SNMP Trap Inform Mode [enable|disable]
132. Security Switch SNMP Trap Inform Timeout [<timeout>]
133. Security Switch SNMP Trap Inform Retry Times [<retries>]
134. Security Switch SNMP Trap Probe Security Engine ID [enable|disable]
135. Security Switch SNMP Trap Security Engine ID [<engineid>]
136. Security Switch SNMP Trap Security Name [<security_name>]
137. Security Switch SNMP Engine ID [<engineid>]
138. Security Switch SNMP Community Add <community> [<ip_addr>] [<ip_mask>]
139. Security Switch SNMP Community Delete <index>
140. Security Switch SNMP Community Lookup [<index>]
141. Security Switch SNMP User Add <engineid> <user_name> [MD5|SHA] [<auth_password>] [DES] [<priv_password>]
142. Security Switch SNMP User Delete <index>
143. Security Switch SNMP User Changekey <engineid> <user_name> <auth_password> [<priv_password>]
144. Security Switch SNMP User Lookup [<index>]
145. Security Switch SNMP Group Add <security_model> <security_name> <group_name>
146. Security Switch SNMP Group Delete <index>
147. Security Switch SNMP Group Lookup [<index>]
148. Security Switch SNMP View Add <view_name> [included|excluded] <oid_subtree>
149. Security Switch SNMP View Delete <index>
150. Security Switch SNMP View Lookup [<index>]
151. Security Switch SNMP Access Add <group_name> <security_model> <security_level> [<read_view_name>] [<write_view_name>]
152. Security Switch SNMP Access Delete <index>
153. Security Switch SNMP Access Lookup [<index>]
154. Security Switch RMON : Remote Network Monitoring

Network : Network security command groups

Security Network Psec : Port Security Status commands

155. Security Network Psec Switch [<port_list>]
156. Security Network Psec Port [<port_list>]

Security Network Limit : Port Security Limit Control commands

157. Security Network Limit Configuration [<port_list>]
158. Security Network Limit Mode [enable|disable]
159. Security Network Limit Aging [enable|disable]
160. Security Network Limit Agetime [<age_time>]
161. Security Network Limit Port [<port_list>] [enable|disable]
162. Security Network Limit Limit [<port_list>] [<limit>]
163. Security Network Limit Action [<port_list>] [none|trap|shut|trap_shut]
164. Security Network Limit Reopen [<port_list>]

Security Network NAS : Network Access Server (IEEE 802.1X) commands

165. Security Network NAS Configuration [<port_list>]
166. Security Network NAS Mode [enable|disable]
167. Security Network NAS State [<port_list>] [auto|authorized|unauthorized|single|multi|macbased]
168. Security Network NAS Reauthentication [enable|disable]
169. Security Network NAS ReauthPeriod [<reauth_period>]
170. Security Network NAS EapolTimeout [<eapol_timeout>]
171. Security Network NAS Agetime [<age_time>]
172. Security Network NAS Holdtime [<hold_time>]
173. Security Network NAS RADIUS_QoS [global|<port_list>] [enable|disable]
174. Security Network NAS RADIUS_VLAN [global|<port_list>] [enable|disable]
175. Security Network NAS Guest_VLAN [global|<port_list>] [enable|disable] [<vid>] [<reauth_max>] [<allow_if_eapol_seen>]
176. Security Network NAS Authenticate [<port_list>] [now]

177. Security Network NAS Statistics [<port_list>] [clear|eapol|radius]

Security Network ACL : Access Control List commands

178. Security Network ACL Configuration [<port_list>]

179. Security Network ACL Action [<port_list>] [permit|deny] [<rate_limiter>] [<evc_policer>] [<port_redirect>] [<mirror>] [<logging>] [<shutdown>]

180. Security Network ACL Policy [<port_list>] [<policy>]

181. Security Network ACL Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]

182. Security Network ACL Add [<ace_id>] [<ace_id_next>]
 [(port <port_list>)] [(policy <policy> <policy_bitmask>)]
 [<tagged>] [<vid>] [<tag_prio>] [<dmac_type>]
 [(etype [<etype>] [<smac>] [<dmac>]) |
 (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>)] |
 (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>)] |
 (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>)] |
 (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>)] |
 (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])]
 [permit|deny] [<rate_limiter>] [<evc_policer>] [<port_redirect>] [<mirror>] [<logging>]
 [<shutdown>]

183. Security Network ACL Delete <ace_id>

184. Security Network ACL Lookup [<ace_id>]

185. Security Network ACL Clear

Security Network ACL Status [combined|static|link_oam|loop_protect|dhcp|ptp|arp_ inspection|mep|ipmc|ip_source_guard|conflicts]

186. Security Network ACL Port State [<port_list>] [enable|disable]

Security Network DHCP : Dynamic Host Configuration Protocol commands

187. Security Network DHCP Relay Configuration

188. Security Network DHCP Relay Mode [enable|disable]

189. Security Network DHCP Relay Server [<ip_addr>]

190. Security Network DHCP Relay Information Mode [enable|disable]

191. Security Network DHCP Relay Information Policy [replace|keep|drop]

192. Security Network DHCP Relay Statistics [clear]

193. Security Network DHCP Snooping Configuration

194. Security Network DHCP Snooping Mode [enable|disable]

195. Security Network DHCP Snooping Port Mode [<port_list>] [trusted|untrusted]

196. Security Network DHCP Snooping Statistics [<port_list>] [clear]

Security Network IP : IP Source Guard commands

197. Security Network IP Source Guard Configuration

198. Security Network IP Source Guard Mode [enable|disable]

199. Security Network IP Source Guard Port Mode [<port_list>] [enable|disable]

200. Security Network IP Source Guard limit [<port_list>] [<dynamic_entry_limit>|unlimited]

201. Security Network IP Source Guard Entry [<port_list>] add|delete
 <vid> <allowed_ip> <allowed_mac>

202. Security Network IP Source Guard Status [<port_list>]

203. Security Network IP Source Guard Translation

Security Network ARP : Address Resolution Protocol commands

204. Security Network ARP Inspection Configuration

205. Security Network ARP Inspection Mode [enable|disable]

206. Security Network ARP Inspection Port Mode [<port_list>] [enable|disable]

207. Security Network ARP Inspection Entry [<port_list>] add|delete
 <vid> <allowed_mac> <allowed_ip>

208. Security Network ARP Inspection Status [<port_list>]

209. Security Network ARP Inspection Translation

AAA : Authentication, Authorization and Accounting commands

210. Security AAA Configuration

211. Security AAA Timeout [<timeout>]

212. Security AAA Deadtime [<dead_time>]

- 213. Security AAA RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]
- 214. Security AAA ACCT_RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]
- 215. Security AAA TACACS+ [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]
- 216. Security AAA Statistics [<server_index>]

STP Commands

- 217. STP Configuration
- 218. STP Version [<stp_version>]
- 219. STP Txhold [<holdcount>]
- 220. STP MaxHops [<maxhops>]
- 221. STP MaxAge [<max_age>]
- 222. STP FwdDelay [<delay>]
- 223. STP CName [<config-name>] [<integer>]
- 224. STP bpduFilter [enable|disable]
- 225. STP bpduGuard [enable|disable]
- 226. STP recovery [<timeout>]
- 227. STP Status [<msti>] [<stp_port_list>]
- 228. STP Msti Priority [<msti>] [<priority>]
- 229. STP Msti Map [<msti>] [clear]
- 230. STP Msti Add <msti> <vid-range>
- 231. STP Port Configuration [<stp_port_list>]
- 232. STP Port Mode [<stp_port_list>] [enable|disable]
- 233. STP Port Edge [<stp_port_list>] [enable|disable]
- 234. STP Port AutoEdge [<stp_port_list>] [enable|disable]
- 235. STP Port P2P [<stp_port_list>] [enable|disable|auto]
- 236. STP Port RestrictedRole [<stp_port_list>] [enable|disable]
- 237. STP Port RestrictedTcn [<stp_port_list>] [enable|disable]
- 238. STP Port bpduGuard [<stp_port_list>] [enable|disable]
- 239. STP Port Statistics [<stp_port_list>] [clear]
- 240. STP Port Mcheck [<stp_port_list>]
- 241. STP Msti Port Configuration [<msti>] [<stp_port_list>]
- 242. STP Msti Port Cost [<msti>] [<stp_port_list>] [<path_cost>]
- 243. STP Msti Port Priority [<msti>] [<stp_port_list>] [<priority>]

Aggr Commands

- 244. Aggr Configuration
- 245. Aggr Add <port_list> [<aggr_id>]
- 246. Aggr Delete <aggr_id>
- 247. Aggr Lookup [<aggr_id>]
- 248. Aggr Mode [smac|dmac|ip|port] [enable|disable]

LACP Commands

- 249. LACP Configuration [<port_list>]
- 250. LACP Mode [<port_list>] [enable|disable]
- 251. LACP Key [<port_list>] [<key>]
- 252. LACP Prio [<port_list>] [<prio>]
- 253. LACP System Prio [<sysprio>]
- 254. LACP Role [<port_list>] [active|passive]
- 255. LACP Status [<port_list>]
- 256. LACP Statistics [<port_list>] [clear]
- 257. LACP Timeout [<port_list>] [fast|slow]

LLDP Commands

- 258. LLDP Configuration [<port_list>]
- 259. LLDP Mode [<port_list>] [enable|disable|rx|tx]
- 260. LLDP Optional_TLV [<port_list>] [port_descr|sys_name|sys_descr|sys_capa|mgmt_addr] [enable|disable]
- 261. LLDP Interval [<interval>]
- 262. LLDP Hold [<hold>]
- 263. LLDP Delay [<delay>]
- 264. LLDP Reinit [<reinit>]
- 265. LLDP Statistics [<port_list>] [clear]
- 266. LLDP Info [<port_list>]
- 267. LLDP cdp_aware [<port_list>] [enable|disable]

Thermal Commands

- 268. Thermal prio_temp [<prio_list>] [<shut_down_temp>]
- 269. Thermal port_prio [<port_list>] [<prio>]
- 270. Thermal status
- 271. Thermal configuration

EVC Commands

- 287. EVC Configuration [<port_list>] [<policer_id>]
- 288. EVC Port DEI [<port_list>] [<dei_mode>]
- 289. EVC Port Tag [<port_list>] [<tag_mode>]
- 290. EVC Port Addr [<port_list>] [<addr_mode>]
- 291. EVC Port L2CP [<port_list>] [<l2cp_list>] [<mode>]
- 292. EVC Policer [<policer_id>] [enable|disable] [<policer_mode>] [<cir>] [<cbs>] [<eir>] [<ebs>]
- 293. EVC Add <evc_id> [<vid>] [<ivid>] [<nni_list>] [<learning>] [inner] [<it_type>] [<it_vid_mode>] [<it_vid>] [<it_preserve>] [<it_pcp>] [<it_dei>] [outer] [<ot_vid>]
- 294. EVC Delete <evc_id>
- 295. EVC Lookup [<evc_id>]
- 296. EVC Status [<evc_id>]
- 297. EVC Statistics [<port_list>] [<class_list>] [<command>]
- 298. EVC ECE Add [<ece_id>] [<ece_id_next>] [uni] [<uni_list>] [<dmac_type>] [<smac>] [tag] [<tag_type>] [<vid>] [<pcp>] [<dei>] [all] (ipv4 [<proto>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) | (ipv6 [<proto>] [<sip_v6>] [<dscp>] [<sport>] [<dport>]) [direction] [<direction>] [evc] [<evc_id>]

- [pop] [<pop>]
- [policy] [<policy>]
- [class] [<class>]
- [outer] [<ot_mode>] [<ot_preserve>] [<ot_pcp>] [<ot_dei>]
- 299. EVC ECE Delete <ece_id>
- 300. EVC ECE Lookup [<ece_id>]
- 301. EVC ECE Status [<ece_id>]

EPS Commands

- 302. EPS create [<inst>] [domport] [1p1|1f1] [<flow_w>] [<flow_p>] [<mep_w>] [<mep_p>] [<mep_aps>] [enable|disable]
- 303. EPS config [<inst>] [aps|noaps] [revert|norevert] [unidir|bidir] [w0s|w10s|w30s|w1m|w5m|w12m] [h0s|h100ms|h500ms|h1s|h2s|h5s|h10s]
- 304. EPS command [<inst>] [clear|lockout|forced|manualp|manualw|exercise|freeze|lockoutlocal]
- 305. EPS state [<inst>]

MEP Commands

- 306. MEP config [<inst>] [mep|mip] [down|up] [<port>] [domport|domevc] [<level>] [itu|ieee] [<meg>] [<mep>] [<vid>] [<flow>] [enable|disable]
- 307. MEP peer MEP [<inst>] [<mep>] [<mac_addr>] [enable|disable]
- 308. MEP cc config [<inst>] [<prio>] [300s|100s|10s|1s|6m|1m|6h] [enable|disable]
- 309. MEP lm config [<inst>] [<prio>] [uni|multi] [single|dual] [10s|1s|6m|1m|6h] [<flr>] [enable|disable]
- 310. MEP aps config [<inst>] [<prio>] [uni|multi] [laps|raps] [<octet>] [enable|disable]
- 311. MEP client config [<inst>] [domport|domevc] [<level>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>]
- 312. MEP ais config [<inst>] [<prio>] [1s|1m] [set|clear] [enable|disable]
- 313. MEP lck config [<inst>] [<prio>] [1s|1m] [enable|disable]
- 314. MEP lt config [<inst>] [<prio>] [<mac_addr>] [<mep>] [<ttl>] [enable|disable]
- 315. MEP lb config [<inst>] [set|clear] [<prio>] [uni|multi] [<mac_addr>] [<mep>] [<tosend>] [<size>] [<gap>] [enable|disable]
- 316. MEP dm config [<inst>] [<prio>] [uni|multi] [<mep>] [oneway|two-way] [std|prop] [rdtrp|flow] [<gap>] [<count>] [us|ns] [keep|reset] [d2ford1] [enable|disable]
- 317. MEP tst config [<inst>] [set|clear] [<prio>] [<mep>] [no_seq|seq] [<rate>] [<size>] [allzero|allone|onezero] [enable|disable]
- 318. MEP state [<inst>]
- 319. MEP lm state [<inst>]
- 320. MEP lm clear <inst>
- 321. MEP lt state [<inst>]
- 322. MEP lb state [<inst>]
- 323. MEP dm state [<inst>]
- 324. MEP dm clear <inst>
- 325. MEP tst state [<inst>]
- 326. MEP tst clear <inst>
- 327. MEP tst clear <inst>

QoS Commands

- 328. QoS Configuration [<port_list>]
- 329. QoS Port Classification Class [<port_list>] [<class>]
- 330. QoS Port Classification DPL [<port_list>] [<dpl>]
- 331. QoS Port Classification PCP [<port_list>] [<pcp>]
- 332. QoS Port Classification DEI [<port_list>] [<dei>]
- 333. QoS Port Classification Tag [<port_list>] [enable|disable]
- 334. QoS Port Classification Map [<port_list>] [<pcp_list>] [<dei_list>] [<class>] [<dpl>]
- 335. QoS Port Classification DSCP [<port_list>] [enable|disable]
- 336. QoS Port Policer Mode [<port_list>] [enable|disable]
- 337. QoS Port Policer Rate [<port_list>] [<rate>]

- 338. QoS Port Policer Unit [<port_list>] [kbps|fps]
- 339. QoS Port Policer FlowControl [<port_list>] [enable|disable]
- 340. QoS Port QueuePolicer Mode [<port_list>] [<queue_list>] [enable|disable]
- 341. QoS Port QueuePolicer Rate [<port_list>] [<queue_list>] [<bit_rate>]
- 342. QoS Port Scheduler Mode [<port_list>] [strict|weighted]
- 343. QoS Port Scheduler Weight [<port_list>] [<queue_list>] [<weight>]
- 344. QoS Port Shaper Mode [<port_list>] [enable|disable]
- 345. QoS Port Shaper Rate [<port_list>] [<bit_rate>]
- 346. QoS Port QueueShaper Mode [<port_list>] [<queue_list>] [enable|disable]
- 347. QoS Port QueueShaper Rate [<port_list>] [<queue_list>] [<bit_rate>]
- 348. QoS Port QueueShaper Excess [<port_list>] [<queue_list>] [enable|disable]
- 349. QoS Port TagRemarking Mode [<port_list>] [classified|default|mapped]
- 350. QoS Port TagRemarking PCP [<port_list>] [<pcp>]
- 351. QoS Port TagRemarking DEI [<port_list>] [<dei>]
- 352. QoS Port TagRemarking Map [<port_list>] [<class_list>] [<dpl_list>] [<pcp>] [<dei>]
- 353. QoS Port DSCP Translation [<port_list>] [enable|disable]
- 354. QoS Port DSCP Classification [<port_list>] [none|zero|selected|all]
- 355. QoS Port DSCP Classification [<port_list>] [none|zero|selected|all]dp_aware]
- 356. QoS DSCP Map [<dscp_list>] [<class>] [<dpl>]
- 357. QoS DSCP Translation [<dscp_list>] [<trans_dscp>]
- 358. QoS DSCP Trust [<dscp_list>] [enable|disable]
- 359. QoS DSCP Classification Mode [<dscp_list>] [enable|disable]
- 360. QoS DSCP Classification Map [<class_list>] [<dpl_list>] [<dscp>]
- 361. QoS DSCP EgressRemap [<dscp_list>] [<dpl_list>] [<dscp>]
- 362. QoS Storm Unicast [enable|disable] [<packet_rate>]
- 363. QoS Storm Multicast [enable|disable] [<packet_rate>]
- 364. QoS Storm Broadcast [enable|disable] [<packet_rate>]
- 365. QoS QCL Add [<qce_id>] [<qce_id_next>]
 [<port_list>]
 [<tag>] [<vid>] [<pcp>] [<dei>] [<smac>] [<dmac_type>]
 [(etype [<etype>]) |
 (LLC [<DSAP>] [<SSAP>] [<control>]) |
 (SNAP [<PID>]) |
 (ipv4 [<protocol>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) |
 (ipv6 [<protocol>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])]
 [<class>] [<dp>] [<classified_dscp>]
- 366. QoS QCL Delete <qce_id>
- 367. QoS QCL Lookup [<qce_id>]
- 368. QoS QCL status [combined|static|conflicts]
- 369. QoS QCL refresh
- 370. QoS QCL refresh

Mirror Commands

- 377. Mirror Configuration [<port_list>]
- 378. Mirror Port [<port>|disable]
- 379. Mirror Mode [<port_list>] [enable|disable|rx|tx]

Firmware Commands

- 380. Firmware Load <ip_addr_string> <file_name> [<activate>]
- 381. Firmware IPv6 Load <ipv6_server> <file_name> [<activate>]
- 382. Firmware Information
- 383. Firmware Swap
- 384. Firmware Peripheral Load <hostname> <file_name>
- 385. Firmware Peripheral Version

MVR Commands

- 384. MVR Configuration
- 385. MVR Mode [enable|disable]
- 386. MVR VLAN Setup [<mvid>] [add|del|upd] [(Name <mvr_name>)]
- 387. MVR VLAN Mode [<vid>|<mvr_name>] [dynamic|compatible]
- 388. MVR VLAN Port [<vid>|<mvr_name>] [<port_list>] [source|receiver|inactive]
- 389. MVR VLAN LLQI [<vid>|<mvr_name>] [mvr_param_llqi]
- 390. MVR VLAN Channel [<vid>|<mvr_name>] [add|del|upd] [channel] [channel_bound] [(Name <grp_name>)]
- 391. MVR VLAN Priority [<vid>|<mvr_name>] [priority] [tagged|untagged]
- 392. MVR Immediate Leave [<port_list>] [enable|disable]
- 393. MVR Status [<vid>] [clear]
- 394. MVR Groups [<vid>]
- 395. MVR SFM [<vid>] [<port_list>]

PTP Commands

- 396. PTP Configuration [<clockinst>]
- 397. PTP PortState <clockinst> [<port_list>] [enable|disable|internal]
- 398. PTP ClockCreate <clockinst> [<devtype>] [<twostep>] [<protocol>] [<oneway>] [<clockid>] [<tag_enable>] [<vid>] [<prio>]
- 400. PTP ClockDelete <clockinst> [<devtype>]
- 401. PTP DefaultDS <clockinst> [<priority1>] [<priority2>] [<domain>]
- 402. PTP CurrentDS <clockinst>
- 403. PTP ParentDS <clockinst>
- 404. PTP Timingproperties <clockinst> [<utcoffset>] [<valid>] [<leap59>] [<leap61>] [<timetrac>] [<freqtrac>] [<ptptimescale>] [<timesource>]
- 405. PTP PortDataSet <clockinst> [<port_list>] [<announceintv>] [<announceto>] [<syncintv>] [<delaymech>] [<minpdelayreqintv>] [<delayasymmetry>] [<ingressLatency>][<egressLatency>]
- 406. PTP LocalClock <clockinst> [update|show|ratio] [<clockratio>]
- 407. PTP Filter <clockinst> [<def_delay_filt>] [<period>] [<dist>]
- 408. PTP Servo <clockinst> [<displaystates>] [<ap_enable>] [<ai_enable>] [<ad_enable>] [<ap>] [<ai>] [<ad>]
- 409. PTP SlaveTableUnicast <clockinst>
- 410. PTP UniConfig <clockinst> [<index>] [<duration>] [<ip_addr>]
- 411. PTP ForeignMasters <clockinst> [<port_list>]
- 412. PTP EgressLatency [show|clear]
- 413. PTP MasterTableUnicast <clockinst>
- 414. PTP ExtClock Output Mode [<ext_clock_enable>] [<clockfreq_out>]
- 415. PTP ExtClock Input Mode [<ext_clock_enable>] [<clockfreq_in>]
- 416. PTP ExtClock Impedance [<impedance>]
- 417. PTP ExtClock Input Status [<clear>]
- 418. PTP Wireless mode <clockinst> [<port_list>] [enable|disable]
- 419. PTP Wireless pre notification <clockinst> <port_list>
- 420. PTP Wireless delay <clockinst> [<port_list>] [<base_delay>] [<incr_delay>]

ERPS Commands

- 421. Erps command [fs|ms|clear] <port> <group-id>
- 422. Erps version [v1|v2] <group-id>
- 423. Erps add <group-id> <east_port> <west_port> [major|sub] [interconnected] [virtual_channel] [<major-ring-id>]
- 424. Erps reversion [revertive|nonrevertive] <group-id>
- 425. Erps vlan add <vid> <group-id>
- 426. Erps vlan delete <vid> <group-id>
- 427. Erps mep <east_sf_mep> <west_sf_mep> <east_raps_mep> <west_raps_mep> <group-id>
- 428. Erps rpl neighbour <rpl_port> <group-id>
- 429. Erps rpl owner <rpl_port> <group-id>
- 430. Erps rpl neighbour clear <group-id>
- 431. Erps rpl owner clear <group-id>
- 432. Erps hold off timeout <hold_timeout> <group-id>
- 433. Erps guard-timeout <guard_timeout> <group-id>
- 434. Erps wtr-timeout <wtr_timeout> <group-id>
- 435. Erps delete <group-id>
- 436. Erps topologychange [propagate|nopropagate] <group-id>
- 437. Erps configuration [<group-id>] [statistics|clear]

LOAM Commands

- 438. LOAM Control [<port_list>] [enable|disable]
- 439. LOAM Mode [<port_list>] [active|passive]
- 440. LOAM Mib-retrieval-support [<port_list>] [enable|disable]
- 441. LOAM Variable-retrieve [<port_list>] [local-info|remote-info]
- 442. LOAM Remote_loopback_support [<port_list>] [enable|disable]
- 443. LOAM Remote_loopback_oper [<port_list>] [enable|disable]
- 444. LOAM Link_monitoring_support [<port_list>] [enable|disable]
- 445. LOAM Frame_error_event [<port_list>] [<error_window>] [<error_threshold>]
- 446. LOAM Symbol_period_error_event [<port_list>] [<error_window>] [<error_threshold>]
- 447. LOAM Frame_error_seconds_summary_event [<port_list>] [<error_window>] [<error_threshold>]
- 448. LOAM Status [<port_list>]
- 449. LOAM Link_monitor_status [<port_list>]
- 450. LOAM Statistics [<port_list>] [clear]

IPMC Commands

- 451. IPMC Configuration [mld|igmp]
- 452. IPMC Mode [mld|igmp] [enable|disable]
- 453. IPMC Flooding [mld|igmp] [enable|disable]
- 454. IPMC Leave Proxy [mld|igmp] [enable|disable]
- 455. IPMC Proxy [mld|igmp] [enable|disable]
- 456. IPMC SSM [mld|igmp] [(Range <prefix> <mask_len>)]
- 457. IPMC State [mld|igmp] [<vid>] [enable|disable]
- 458. IPMC Querier [mld|igmp] [<vid>] [enable|disable]
- 459. IPMC Compatibility [mld|igmp] [<vid>] [auto|v1|v2|v3]
- 460. IPMC Fastleave [mld|igmp] [<port_list>] [enable|disable]
- 461. IPMC Throttling [mld|igmp] [<port_list>] [limit_group_number]
- 462. IPMC Filtering [mld|igmp] [<port_list>] [add|del] [group_addr]
- 463. IPMC Router [mld|igmp] [<port_list>] [enable|disable]
- 464. IPMC Status [mld|igmp] [<vid>]
- 465. IPMC Groups [mld|igmp] [<vid>]
- 466. IPMC Version [mld|igmp] [<vid>]
- 467. IPMC VLAN Add [mld|igmp] <vid>

- 468. IPMC VLAN Delete [mld|igmp] <vid>
- 469. IPMC SFM [mld|igmp] [<vid>] [<port_list>]
- 470. IPMC Parameter RV [mld|igmp] [<vid>] [ipmc_param_rv]
- 471. IPMC Parameter QI [mld|igmp] [<vid>] [ipmc_param_qi]
- 472. IPMC Parameter QRI [mld|igmp] [<vid>] [ipmc_param_qri]
- 473. IPMC Parameter LLQI [mld|igmp] [<vid>] [ipmc_param_llqi]
- 474. IPMC Parameter URI [mld|igmp] [<vid>] [ipmc_param_uri]

sFlow Commands

- 475. sFlow Configuration
- 476. sFlow Receiver [release] [<timeout>] [<ip_addr_host>] [<udp_port>] [<datagram_size>]
- 477. sFlow FlowSampler [<port_list>] [<sampling_rate>] [<max_hdr_size>]
- 478. sFlow CounterPoller [<port_list>] [<interval>]
- 479. sFlow Statistics Receiver [clear]
- 480. sFlow Statistics Samplers [<port_list>] [clear]

VCL Commands

- 481. VCL Macvlan Configuration
- 482. VCL Macvlan Add <mac_addr> <vid> [<port_list>]
- 483. VCL Macvlan Del <mac_addr>
- 484. VCL Status [combined|static|nas|all]
- 485. VCL ProtoVlan Protocol Add Eth2 <ether_type>|arp|ip|ipx|at <group_id>
- 486. VCL ProtoVlan Protocol Add Snap <oui>|rfc_1042|snap_8021h <pid> <group_id>
- 487. VCL ProtoVlan Protocol Add Llc <dsap> <ssap> <group_id>
- 488. VCL ProtoVlan Protocol Delete Eth2 <ether_type>|arp|ip|ipx|at
- 489. VCL ProtoVlan Protocol Delete Snap <oui>|rfc_1042|snap_8021h <pid>
- 490. VCL ProtoVlan Protocol Delete Llc <dsap> <ssap>
- 491. VCL ProtoVlan Vlan Add [<port_list>] <group_id> <vid>
- 492. VCL ProtoVlan Vlan Delete [<port_list>] <group_id>
- 493. VCL ProtoVlan Conf
- 494. VCL IPvlan Configuration [<vce_id>]
- 495. VCL IPvlan Add [<vce_id>] <ip_addr_mask> <vid> [<port_list>]
- 496. VCL IPvlan Delete <vce_id>

EtherSAT Loopback Commands

See the RFC2544 Performance Tests User Guide, 33540 for the EtherSAT Loopback configuration commands.

Static Routing (SIR) Commands

See the Static IP Routing (SIR) User Guide, 33542 for the SIR (Static IP Routing) commands.

< end of list>

Alphabetical List of S3280 CLI Commands

A

1. Aggr Configuration
2. Aggr Add <port_list> [<aggr_id>]
3. Aggr Delete <aggr_id>
4. Aggr Lookup [<aggr_id>]
5. Aggr Mode [smac|dmac|ip|port] [enable|disable]

C

6. Config Backup Binary <hostname> <file_name>
7. Config Restore Binary <hostname> <file_name>
8. Config Default [keep_ip]

E

9. EPS create [<inst>] [domport] [1p1|1f1] [<flow_w>] [<flow_p>] [<mep_w>] [<mep_p>] [<mep_aps>] [enable|disable]
10. EVC Configuration [<port_list>] [<policer_id>]
11. EPS config [<inst>] [aps|noaps] [revert|norevert] [unidir|bidir] [w0s|w10s|w30s|w1m|w5m|w12m] [h0s|h100ms|h500ms|h1s|h2s|h5s|h10s]
12. Erps command [fs|ms|clear] <port> <group-id>
13. Erps version [v1|v2] <group-id>
14. EVC Port DEI [<port_list>] [<dei_mode>]
15. EPS command [<inst>] [clear|lockout|forced|manualp|manualw|exercise|freeze|lockoutlocal]
16. Erps add <group-id> <east_port> <west_port> [major|sub] [interconnected] [virtual_channel] [<major-ring-id>]
17. EVC Port Tag [<port_list>] [<tag_mode>]
18. EPS state [<inst>]
19. EVC Port Addr [<port_list>] [<addr_mode>]
20. Erps reversion [revertive|nonrevertive] <group-id>
21. EVC Port L2CP [<port_list>] [<l2cp_list>] [<mode>]
22. Erps vlan add <vid> <group-id>
23. EVC Policer [<policer_id>] [enable|disable] [<policer_mode>] [<cir>] [<cbs>] [<eir>] [<ebs>]
24. Erps vlan delete <vid> <group-id>
25. EVC Add <evc_id> [<vid>] [<ivid>] [<nni_list>] [<learning>] [inner] [<it_type>] [<it_vid_mode>] [<it_vid>] [<it_preserve>] [<it_pcp>] [<it_dei>] [outer] [<ot_vid>]
26. Erps mep <east_sf_mep> <west_sf_mep> <east_raps_mep> <west_raps_mep> <group-id>
27. EVC Delete <evc_id>
28. Erps rpl neighbour <rpl_port> <group-id>
29. Erps rpl owner <rpl_port> <group-id>
30. EVC Lookup [<evc_id>]
31. EVC Status [<evc_id>]
32. Erps rpl neighbour clear <group-id>
33. Erps rpl owner clear <group-id>
34. EVC Statistics [<port_list>] [<class_list>] [<command>]
35. Erps hold off timeout <hold_timeout> <group-id>
36. Erps guard-timeout <guard_timeout> <group-id>
37. EVC ECE Add [<ece_id>] [<ece_id_next>] [uni] [<uni_list>] [<dmac_type>] [<smac>] [tag] [<tag_type>] [<vid>] [<pcp>] [<dei>] [all] (ipv4 [<proto>] [<sip>] [<dsdp>] [<fragment>] [<sport>] [<dport>]) |

- (ipv6 [<proto>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])
 - [direction] [<direction>]
 - [evc] [<evc_id>]
 - [pop] [<pop>]
 - [policy] [<policy>]
 - [class] [<class>]
 - [outer] [<ot_mode>] [<ot_preserve>] [<ot_pcp>] [<ot_dei>]
38. Erps wtr-timeout <wtr_timeout> <group-id>
 39. EVC ECE Delete <ece_id>
 40. Erps delete <group-id>
 41. EVC ECE Lookup [<ece_id>]
 42. Erps topologychange [propagate|nopropagate] <group-id>
 43. EVC ECE Status [<ece_id>]
 44. Erps configuration [<group-id>] [statistics|clear]
 45. EtherSAT Loopback Commands – see the related manual

F

46. Firmware Load <ip_addr_string> <file_name> [<activate>]
47. Firmware IPv6 Load <ipv6_server> <file_name> [<activate>]
48. Firmware Information
49. Firmware Swap
50. Firmware Peripheral Load <hostname> <file_name>
51. Firmware Peripheral Version

H

52. Help

I

53. IP ARP Show
54. IP Configuration
55. IPMC Configuration [mld|igmp]
56. IP DHCP [enable|disable]
57. IPMC Mode [mld|igmp] [enable|disable]
58. IP Setup [<ip_addr>] [<ip_mask>] [<ip_router>]
59. IPMC Flooding [mld|igmp] [enable|disable]
60. IP Ping <ip_addr_string> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)]
61. IPMC Leave Proxy [mld|igmp] [enable|disable]
62. IP DNS [<ip_addr>]
63. IPMC Proxy [mld|igmp] [enable|disable]
64. IP DNS_Proxy [enable|disable]
65. IPMC SSM [mld|igmp] [(Range <prefix> <mask_len>)]
66. IPMC State [mld|igmp] [<vid>] [enable|disable]
67. IP IPv6 AUTOCONFIG [enable|disable]
68. IPMC Querier [mld|igmp] [<vid>] [enable|disable]
69. IP IPv6 Setup [<ipv6_addr>] [<ipv6_prefix>] [<ipv6_router>]
70. IP IPv6 State <ipv6_addr> [enable|disable]
71. IPMC Compatibility [mld|igmp] [<vid>] [auto|v1|v2|v3]
72. IP IPv6 Ping6 <ipv6_addr> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)]
73. IPMC Fasteave [mld|igmp] [<port_list>] [enable|disable]
74. IPMC Throttling [mld|igmp] [<port_list>] [limit_group_number]
75. IPMC Filtering [mld|igmp] [<port_list>] [add|del] [group_addr]
76. IPMC Router [mld|igmp] [<port_list>] [enable|disable]
77. IPMC Status [mld|igmp] [<vid>]

- 78. IPMC Groups [mld|igmp] [<vid>]
- 79. IPMC Version [mld|igmp] [<vid>]
- 80. IPMC VLAN Add [mld|igmp] <vid>
- 81. IPMC VLAN Delete [mld|igmp] <vid>
- 82. IPMC SFM [mld|igmp] [<vid>] [<port_list>]
- 83. IPMC Parameter RV [mld|igmp] [<vid>] [ipmc_param_rv]
- 84. IPMC Parameter QI [mld|igmp] [<vid>] [ipmc_param_qi]
- 85. IPMC Parameter QRI [mld|igmp] [<vid>] [ipmc_param_qri]
- 86. IPMC Parameter LLQI [mld|igmp] [<vid>] [ipmc_param_llqi]
- 87. IPMC Parameter URI [mld|igmp] [<vid>] [ipmc_param_uri]
- 88. IP MVlan [<vid>]
- 89. IP NTP Configuration
- 90. IP NTP Mode [enable|disable]
- 91. IP NTP Server Add <server_index> <ip_addr_string>
- 92. IP NTP Server Ipv6 Add <server_index> <server_ipv6>
- 93. IP NTP Server Delete <server_index>

L

- 94. LACP Configuration [<port_list>]
- 95. LLDP Configuration [<port_list>]
- 96. LOAM Control [<port_list>] [enable|disable]
- 97. Loop Protect Configuration
- 98. LACP Mode [<port_list>] [enable|disable]
- 99. LLDP Mode [<port_list>] [enable|disable|rx|tx]
- 100. LOAM Mode [<port_list>] [active|passive]
- 101. Loop Protect Mode [enable|disable]
- 102. LACP Key [<port_list>] [<key>]
- 103. LLDP Optional_TLV [<port_list>] [port_descr|sys_name|sys_descr|sys_capa|mgmt_addr] [enable|disable]
- 104. LOAM Mib-retrival-support [<port_list>] [enable|disable]
- 105. Logout
- 106. Loop Protect Transmit [<transmit-time>]
- 107. LACP Prio [<port_list>] [<prio>]
- 108. LLDP Interval [<interval>]
- 109. LOAM Variable-retrieve [<port_list>] [local-info|remote-info]
- 110. Loop Protect Shutdown [<shutdown-time>]
- 111. LACP System Prio [<sysprio>]
- 112. LLDP Hold [<hold>]
- 113. LOAM Remote_loopback_support [<port_list>] [enable|disable]
- 114. Loop Protect Port Configuration [<port_list>]
- 115. LACP Role [<port_list>] [active|passive]
- 116. LLDP Delay [<delay>]
- 117. LOAM Remote_loopback_oper [<port_list>] [enable|disable]
- 118. Loop Protect Port Mode [<port_list>] [enable|disable]
- 119. LACP Status [<port_list>]
- 120. LLDP Reinit [<reinit>]
- 121. LOAM Link_monitoring_support [<port_list>] [enable|disable]
- 122. loop protect port action [<port_list>] [shutdown|trap|log|shut_log|shut_trap|log_trap|all]
- 123. LACP Statistics [<port_list>] [clear]
- 124. LLDP Statistics [<port_list>] [clear]
- 125. Loop Protect Port Transmit [<port_list>] [enable|disable]
- 126. LACP Timeout [<port_list>] [fast|slow]
- 127. LLDP Info [<port_list>]
- 128. Loop Protect Status [<port_list>]
- 129. LLDP cdp_aware [<port_list>] [enable|disable]
- 130. LOAM Frame_error_event [<port_list>] [<error_window>] [<error_threshold>]
- 131. LOAM Symbol_period_error_event [<port_list>] [<error_window>] [<error_threshold>]

- 132. LOAM Frame_error_seconds_summary_event [<port_list>] [<error_window>] [<error_threshold>]
- 133. LOAM Status [<port_list>]
- 134. LOAM Link_monitor_status [<port_list>]
- 135. LOAM Statistics [<port_list>] [clear]

M

- 136. MAC Configuration [<port_list>]
- 137. MEP config [<inst>] [mep|mip] [down|up] [<port>] [domport|domevc] [<level>] [itu|ieee] [<meg>] [<mep>] [<vid>] [<flow>] [enable|disable]
- 138. Mirror Configuration [<port_list>]
- 139. MVR Configuration
- 140. MAC Add <mac_addr> <port_list> [<vid>]
- 141. MEP peer MEP [<inst>] [<mep>] [<mac_addr>] [enable|disable]
- 142. Mirror Port [<port>|disable]
- 143. MVR Mode [enable|disable]
- 144. MAC Delete <mac_addr> [<vid>]
- 145. MEP cc config [<inst>] [<prio>] [300s|100s|10s|1s|6m|1m|6h] [enable|disable]
- 146. MVR VLAN Setup [<mvid>] [add|del|upd] [(Name <mvr_name>)]
- 147. MAC Lookup <mac_addr> [<vid>]
- 148. MEP lm config [<inst>] [<prio>] [uni|multi] [single|dual] [10s|1s|6m|1m|6h] [<flr>] [enable|disable]
- 149. Mirror Mode [<port_list>] [enable|disable|rx|tx]
- 150. MVR VLAN Mode [<vid>|<mvr_name>] [dynamic|compatible]
- 151. MAC Agetime [<age_time>]
- 152. MEP aps config [<inst>] [<prio>] [uni|multi] [laps|raps] [<octet>] [enable|disable]
- 153. MVR VLAN Port [<vid>|<mvr_name>] [<port_list>] [source|receiver|inactive]
- 154. MAC Learning [<port_list>] [auto|disable|secure]
- 155. MEP client config [<inst>] [domport|domevc] [<level>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>]
- 156. MVR VLAN LLQI [<vid>|<mvr_name>] [mvr_param_llqi]
- 157. MAC Dump [<mac_max>] [<mac_addr>] [<vid>]
- 158. MEP ais config [<inst>] [<prio>] [1s|1m] [set|clear] [enable|disable]
- 159. MVR VLAN Channel [<vid>|<mvr_name>] [add|del|upd] [channel] [channel_bound] [(Name <grp_name>)]
- 160. MAC Statistics [<port_list>]
- 161. MEP lck config [<inst>] [<prio>] [1s|1m] [enable|disable]
- 162. MVR VLAN Priority [<vid>|<mvr_name>] [priority] [tagged|untagged]
- 163. MAC Flush
- 164. MEP lt config [<inst>] [<prio>] [<mac_addr>] [<mep>] [<ttl>] [enable|disable]
- 165. MVR Immediate Leave [<port_list>] [enable|disable]
- 166. MEP lb config [<inst>] [set|clear] [<prio>] [uni|multi] [<mac_addr>] [<mep>] [<tosend>] [<size>] [<gap>] [enable|disable]
- 167. MVR Status [<vid>] [clear]
- 168. MEP dm config [<inst>] [<prio>] [uni|multi] [<mep>] [oneway|twoway] [std|prop] [rdtrp|flow] [<gap>] [<count>] [us|ns] [keep|reset] [d2ford1] [enable|disable]
- 169. MVR Groups [<vid>]
- 170. MEP tst config [<inst>] [set|clear] [<prio>] [<mep>] [no_seq|seq] [<rate>] [<size>] [allzero|allone|onezero] [enable|disable]
- 171. MVR SFM [<vid>] [<port_list>]
- 172. MEP state [<inst>]
- 173. MEP lm state [<inst>]
- 174. MEP lm clear <inst>
- 175. MEP lt state [<inst>]
- 176. MEP lb state [<inst>]
- 177. MEP dm state [<inst>]
- 178. MEP dm clear <inst>
- 179. MEP tst state [<inst>]

180. MEP tst clear <inst>

P

- 181. Port Configuration [<port_list>] [up|down]
- 182. PTP Configuration [<clockinst>]
- 183. PVLAN Configuration [<port_list>]
- 184. Port Mode [<port_list>] [auto|10hdx|10fdx|100hdx|100fdx|1000fdx|2500fdx|sfp_auto_ams]
- 185. PTP PortState <clockinst> [<port_list>] [enable|disable|internal]
- 186. PVLAN Add <pvlan_id> [<port_list>]
- 187. Port Flow Control [<port_list>] [enable|disable]
- 188. PTP ClockCreate <clockinst> [<devtype>] [<twostep>] [<protocol>] [<oneway>] [<clockid>] [<tag_enable>] [<vid>] [<prio>]
- 189. PVLAN Delete <pvlan_id>
- 191. Port State [<port_list>] [enable|disable]
- 192. PTP ClockDelete <clockinst> [<devtype>]
- 193. PVLAN Lookup [<pvlan_id>]
- 194. Port MaxFrame [<port_list>] [<max_frame>]
- 195. PTP DefaultDS <clockinst> [<priority1>] [<priority2>] [<domain>]
- 196. PVLAN Isolate [<port_list>] [enable|disable]
- 197. Port Power [<port_list>] [enable|disable|actiphy|dynamic]
- 198. PTP CurrentDS <clockinst>
- 199. Port Excessive [<port_list>] [discard|restart]
- 200. PTP ParentDS <clockinst>
- 201. Port Statistics [<port_list>] [<command>] [up|down]
- 202. PTP Timingproperties <clockinst> [<utcoffset>] [<valid>] [<leap59>] [<leap61>] [<timetrac>] [<freqtrac>] [<ptptimescale>] [<timesource>]
- 203. Port VeriPHY [<port_list>]
- 204. PTP PortDataSet <clockinst> [<port_list>] [<announceintv>] [<announceto>] [<syncintv>] [<delaymech>] [<minpdelayreqintv>] [<delayasymmetry>] [<ingressLatency>] [<egressLatency>]
- 205. PTP LocalClock <clockinst> [update|show|ratio] [<clockratio>]
- 206. Port SFP [<port_list>]
- 207. PTP Filter <clockinst> [<def_delay_filt>] [<period>] [<dist>]
- 208. PTP Servo <clockinst> [<displaystates>] [<ap_enable>] [<ai_enable>] [<ad_enable>] [<ap>] [<ai>] [<ad>]
- 209. PTP SlaveTableUnicast <clockinst>
- 210. PTP UniConfig <clockinst> [<index>] [<duration>] [<ip_addr>]
- 211. PTP ForeignMasters <clockinst> [<port_list>]
- 212. PTP EgressLatency [show|clear]
- 213. PTP MasterTableUnicast <clockinst>
- 214. PTP ExtClock Output Mode [<ext_clock_enable>] [<clockfreq_out>]
- 215. PTP ExtClock Input Mode [<ext_clock_enable>] [<clockfreq_in>]
- 216. PTP ExtClock Impedance [<impedance>]
- 217. PTP ExtClock Input Status [<clear>]
- 218. PTP Wireless mode <clockinst> [<port_list>] [enable|disable]
- 219. PTP Wireless pre notification <clockinst> <port_list>
- 220. PTP Wireless delay <clockinst> [<port_list>] [<base_delay>] [<incr_delay>]
- 221. Port DMI Configuration [<port_list>] [<dmi_rx_pwr_int_thr>]
- 222. Port DMI Statistics [<port_list>]
- 223. Port Description [<port_list>] [<name>]

Q

- 224. QoS Configuration [<port_list>]
- 225. QoS Port Classification Class [<port_list>] [<class>]
- 226. QoS Port Classification DPL [<port_list>] [<dpl>]
- 227. QoS Port Classification PCP [<port_list>] [<pcp>]

- 228. QoS Port Classification DEI [<port_list>] [<dei>]
- 229. QoS Port Classification Tag [<port_list>] [enable|disable]
- 230. QoS Port Classification Map [<port_list>] [<pcp_list>] [<dei_list>] [<class>] [<dpl>]
- 231. QoS Port Classification DSCP [<port_list>] [enable|disable]
- 232. QoS Port Policer Mode [<port_list>] [enable|disable]
- 233. QoS Port Policer Rate [<port_list>] [<rate>]
- 234. QoS Port Policer Unit [<port_list>] [kpbs|fps]
- 235. QoS Port Policer FlowControl [<port_list>] [enable|disable]
- 236. QoS Port QueuePolicer Mode [<port_list>] [<queue_list>] [enable|disable]
- 237. QoS Port QueuePolicer Rate [<port_list>] [<queue_list>] [<bit_rate>]
- 238. QoS Port Scheduler Mode [<port_list>] [strict|weighted]
- 239. QoS Port Scheduler Weight [<port_list>] [<queue_list>] [<weight>]
- 240. QoS Port Shaper Mode [<port_list>] [enable|disable]
- 241. QoS Port Shaper Rate [<port_list>] [<bit_rate>]
- 242. QoS Port QueueShaper Mode [<port_list>] [<queue_list>] [enable|disable]
- 243. QoS Port QueueShaper Rate [<port_list>] [<queue_list>] [<bit_rate>]
- 244. QoS Port QueueShaper Excess [<port_list>] [<queue_list>] [enable|disable]
- 245. QoS Port TagRemarking Mode [<port_list>] [classified|default|mapped]
- 246. QoS Port TagRemarking PCP [<port_list>] [<pcp>]
- 247. QoS Port TagRemarking DEI [<port_list>] [<dei>]
- 248. QoS Port TagRemarking Map [<port_list>] [<class_list>] [<dpl_list>] [<pcp>] [<dei>]
- 249. QoS Port DSCP Translation [<port_list>] [enable|disable]
- 250. QoS Port DSCP Classification [<port_list>] [none|zero|selected|all]
- 251. QoS Port DSCP EgressRemark [<port_list>] [disable|enable|remap_dp_unaware|remap_dp_aware]
- 252. QoS DSCP Map [<dscp_list>] [<class>] [<dpl>]
- 253. QoS DSCP Translation [<dscp_list>] [<trans_dscp>]
- 254. QoS DSCP Trust [<dscp_list>] [enable|disable]
- 255. QoS DSCP Classification Mode [<dscp_list>] [enable|disable]
- 256. QoS DSCP Classification Map [<class_list>] [<dpl_list>] [<dscp>]
- 257. QoS DSCP EgressRemap [<dscp_list>] [<dpl_list>] [<dscp>]
- 258. QoS Storm Unicast [enable|disable] [<packet_rate>]
- 259. QoS Storm Multicast [enable|disable] [<packet_rate>]
- 260. QoS Storm Broadcast [enable|disable] [<packet_rate>]
- 261. QoS QCL Add [<qce_id>] [<qce_id_next>]
 - [<port_list>]
 - [<tag>] [<vid>] [<pcp>] [<dei>] [<smac>] [<dmac_type>]
 - [(etype [<etype>]) |
 - (LLC [<DSAP>] [<SSAP>] [<control>)] |
 - (SNAP [<PID>)] |
 - (ipv4 [<protocol>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) |
 - (ipv6 [<protocol>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])
 - [<class>] [<dp>] [<classified_dscp>]
- 262. QoS QCL Delete <qce_id>
- 263. QoS QCL Lookup [<qce_id>]
- 264. QoS QCL status [combined|static|conflicts]
- 265. QoS QCL refresh

S

- 266. Security AAA Configuration
- 267. Security Network ACL Configuration [<port_list>]
- 268. Security Network ARP Inspection Configuration
- 269. Security Network DHCP Relay Configuration
- 270. Security Network IP Source Guard Configuration
- 271. Security Network Limit Configuration [<port_list>]
- 272. Security Network NAS Configuration [<port_list>]
- 273. Security Network Psec Switch [<port_list>]
- 274. Security Switch Access Configuration
- 275. Security Switch HTTPS Configuration
- 276. Security Switch Privilege Level Configuration
- 277. Security Switch RMON Statistics Add <stats_id> <data_source>
- 278. Security Switch SNMP Configuration
- 279. Security Switch SSH Configuration
- 280. Security Switch Users Configuration
- 281. sFlow Configuration
- 282. STP Configuration
- 283. System Configuration [all | (port <port_list>)]
- 284. System Log Configuration
- 285. System Timezone Configuration
- 286. System Version
- 287. Security AAA Timeout [<timeout>]
- 288. Security Network ACL Action [<port_list>] [permit|deny] [<rate_limiter>]
 [<evc_policer>] [<port_redirect>] [<mirror>] [<logging>] [<shutdown>]
- 289. Security Network ARP Inspection Mode [enable|disable]
- 290. Security Network DHCP Relay Mode [enable|disable]
- 291. Security Network IP Source Guard Mode [enable|disable]
- 292. Security Network Limit Mode [enable|disable]
- 293. Security Network NAS Mode [enable|disable]
- 294. Security Network Psec Port [<port_list>]
- 295. Security Switch Access Mode [enable|disable]
- 296. Security Switch HTTPS Mode [enable|disable]
- 297. Security Switch Privilege Level Group <group_name> [<cro>] [<crw>] [<sro>] [<srw>]
- 298. Security Switch RMON Statistics Delete <stats_id>
- 299. Security Switch SNMP Mode [enable|disable]
- 300. Security Switch SSH Mode [enable|disable]
- 301. Security Switch Users Add <user_name> <password> <privilege_level>
- 302. sFlow Receiver [release] [<timeout>] [<ip_addr_host>] [<udp_port>] [<datagram_size>]
- 303. STP Version [<stp_version>]
- 304. System Log Server Mode [enable|disable]
- 305. System Name [<name>]
- 306. System Timezone Offset [<offset>]
- 307. Security AAA Deadtime [<dead_time>]
- 308. Security Network ACL Policy [<port_list>] [<policy>]
- 309. Security Network ARP Inspection Port Mode [<port_list>] [enable|disable]
- 310. Security Network DHCP Relay Server [<ip_addr>]
- 311. Security Network IP Source Guard Port Mode [<port_list>] [enable|disable]
- 312. Security Network Limit Aging [enable|disable]
- 313. Security Network NAS State [<port_list>] [auto|authorized|unauthorized|single|multi|macbased]
- 314. Security Switch Access Add <access_id> <start_ip_addr> <end_ip_addr> [web] [snmp] [telnet]
- 315. Security Switch HTTPS Redirect [enable|disable]
- 316. Security Switch Privilege Level Current
- 317. Security Switch RMON Statistics Lookup [<stats_id>]
- 318. Security Switch SNMP Version [1|2c|3]
- 319. Security Switch Users Delete <user_name>

- 320. sFlow FlowSampler [<port_list>] [<sampling_rate>] [<max_hdr_size>]
- 321. STP Txhold [<holdcount>]
- 322. System Contact [<contact>]
- 323. System Log Server Address [<ip_addr_string>]
- 324. System Timezone Acronym [<acronym>]
- 325. Security AAA RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]
- 326. Security Network ACL Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]
- 327. Security Network ARP Inspection Entry [<port_list>] add|delete <vid> <allowed_mac> <allowed_ip>
- 328. Security Network IP Source Guard limit [<port_list>] [<dynamic_entry_limit>|unlimited]
- 329. Security Network Limit Agetime [<age_time>]
- 330. Security Network NAS Reauthentication [enable|disable]
- 331. Security Switch Access Ipv6 Add <access_id> <start_ipv6_addr> <end_ipv6_addr> [web] [snmp] [telnet]
- 332. Security Switch RMON History Add <history_id> <data_source> [<interval>] [<buckets>]
- 333. Security Switch SNMP Read Community [<community>]
- 334. sFlow CounterPoller [<port_list>] [<interval>]
- 335. STP MaxHops [<maxhops>]
- 336. System DST Configuration
- 337. System Location [<location>]
- 338. System Log Level [info|warning|error]
- 339. Security AAA ACCT_RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]
- 340. Security Network ACL Add [<ace_id>] [<ace_id_next>] [(port <port_list>)] [(policy <policy> <policy_bitmask>)] [<tagged>] [<vid>] [<tag_prio>] [<dmac_type>] [(etype [<etype>] [<smac>] [<dmac>]) | (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) | (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) | (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) | (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) | (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>)))] [permit|deny] [<rate_limiter>] [<evc_policer>] [<port_redirect>] [<mirror>] [<logging>] [<shutdown>]
- 341. Security Network ARP Inspection Status [<port_list>]
- 342. Security Network DHCP Relay Information Mode [enable|disable]
- 343. Security Network IP Source Guard Entry [<port_list>] add|delete <vid> <allowed_ip> <allowed_mac>
- 344. Security Network Limit Port [<port_list>] [enable|disable]
- 345. Security Network NAS ReauthPeriod [<reauth_period>]
- 346. Security Switch Access Delete <access_id>
- 347. Security Switch RMON History Delete <history_id>
- 348. Security Switch SNMP Write Community [<community>]
- 349. sFlow Statistics Receiver [clear]
- 350. STP MaxAge [<max_age>]
- 351. System DST Mode [disable|recurring|non-recurring]
- 352. Security AAA TACACS+ [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]
- 353. Security Network ACL Delete <ace_id>
- 354. Security Network ARP Inspection Translation
- 355. Security Network DHCP Relay Information Policy [replace|keep|drop]
- 356. Security Network IP Source Guard Status [<port_list>]
- 357. Security Network Limit Limit [<port_list>] [<limit>]
- 358. Security Network NAS EapolTimeout [<eapol_timeout>]
- 359. Security Switch Access Lookup [<access_id>]
- 360. Security Switch RMON History Lookup [<history_id>]
- 361. Security Switch SNMP Trap Mode [enable|disable]
- 362. sFlow Statistics Samplers [<port_list>] [clear]
- 363. STP FwdDelay [<delay>]
- 364. System DST start <week> <day> <month> <date> <year> <hour> <minute>
- 365. System Log Lookup [<log_id>] [all|info|warning|error]
- 366. Security Network ACL Lookup [<ace_id>]

- 367. Security Network DHCP Relay Statistics [clear]
- 368. Security Network IP Source Guard Translation
- 369. Security Network Limit Action [<port_list>] [none|trap|shut|trap_shut]
- 370. Security Network NAS Agetime [<age_time>]
- 371. Security Switch Access Clear
- 372. Security Switch Auth Configuration
- 373. Security Switch RMON Alarm Add <alarm_id> <interval> <alarm_variable> [absolute|
- 374. delta] <rising_threshold> <rising_event_index> <falling_threshold> <falling_event_index>
[rising|falling|both]
- 375. Security Switch SNMP Trap Version [1|2c|3]
- 376. STP CName [<config-name>] [<integer>]
- 377. System DST end <week> <day> <month> <date> <year> <hour> <minute>
- 378. System Log Clear [all|info|warning|error]
- 379. System Reboot
- 380. Security Network ACL Clear
- 381. Security Network Limit Reopen [<port_list>]
- 382. Security Network NAS Holdtime [<hold_time>]
- 383. Security Switch Access Statistics [clear]
- 384. Security Switch Auth Method [console|telnet|ssh|web] [none|local|radius|tacacs+] [enable|disable]
- 385. Security Switch RMON Alarm Delete <alarm_id>
- 386. Security Switch SNMP Trap Community [<community>]
- 387. STP bpduFilter [enable|disable]
- 388. System Date
- 389. System DST Offset [<dst_offset>]
- 390. Security AAA Statistics [<server_index>]
- 391. Security Network ACL Status
[combined|static|link_oam|loop_protect|dhcp|ptp|arp_inspection|mep|ipmc|ip_source_guard|conflicts]
- 392. Security Network NAS RADIUS_QoS [global|<port_list>] [enable|disable]
- 393. Security Switch RMON Alarm Lookup [<alarm_id>]
- 394. Security Switch SNMP Trap Destination [<ip_addr_string>]
- 395. STP bpduGuard [enable|disable]
- 396. System PowerSupply Active
- 397. Security Network ACL Port State [<port_list>] [enable|disable]
- 398. Security Network NAS RADIUS_VLAN [global|<port_list>] [enable|disable]
- 399. Security Switch RMON Event Add <event_id> [none|log|trap|log_trap] [<community>] [<description>]
- 400. Security Switch SNMP Trap IPv6 Destination [<ipv6_addr>]
- 401. STP recovery [<timeout>]
- 402. Security Network NAS Guest_VLAN [global|<port_list>] [enable|disable] [<vid>] [<reauth_max>]
[<allow_if_eapol_seen>]
- 403. Security Switch RMON Event Delete <event_id>
- 404. Security Switch SNMP Trap Authentication Failure [enable|disable]
- 405. STP Status [<msti>] [<stp_port_list>]
- 406. Security Network NAS Authenticate [<port_list>] [now]
- 407. Security Switch RMON Event Lookup [<event_id>]
- 408. Security Switch SNMP Trap Link-up [enable|disable]
- 409. STP Msti Priority [<msti>] [<priority>]
- 410. Security Network NAS Statistics [<port_list>] [clear|eapol|radius]
- 411. Security Switch SNMP Trap Inform Mode [enable|disable]
- 412. STP Msti Map [<msti>] [clear]
- 413. Security Switch SNMP Trap Inform Timeout [<timeout>]
- 414. STP Msti Add <msti> <vid-range>
- 415. Security Switch SNMP Trap Inform Retry Times [<retries>]
- 416. STP Port Configuration [<stp_port_list>]
- 417. Security Switch SNMP Trap Probe Security Engine ID [enable|disable]
- 418. STP Port Mode [<stp_port_list>] [enable|disable]
- 419. Security Switch SNMP Trap Security Engine ID [<engineid>]
- 420. STP Port Edge [<stp_port_list>] [enable|disable]
- 421. Security Switch SNMP Trap Security Name [<security_name>]

- 422. STP Port AutoEdge [<stp_port_list>] [enable|disable]
- 423. Security Switch SNMP Engine ID [<engineid>]
- 424. STP Port P2P [<stp_port_list>] [enable|disable|auto]
- 425. Security Switch SNMP Community Add <community> [<ip_addr>] [<ip_mask>]
- 426. STP Port RestrictedRole [<stp_port_list>] [enable|disable]
- 427. Security Switch SNMP Community Delete <index>
- 428. STP Port RestrictedTcn [<stp_port_list>] [enable|disable]
- 429. Security Switch SNMP Community Lookup [<index>]
- 430. STP Port bpduGuard [<stp_port_list>] [enable|disable]
- 431. Security Switch SNMP User Add <engineid> <user_name> [MD5|SHA]
- 432. [<auth_password>] [DES] [<priv_password>]
- 433. STP Port Statistics [<stp_port_list>] [clear]
- 434. Security Switch SNMP User Delete <index>
- 435. STP Port Mcheck [<stp_port_list>]
- 436. Security Switch SNMP User Changekey <engineid> <user_name> <auth_password>
- [<priv_password>]
- 437. STP Msti Port Configuration [<msti>] [<stp_port_list>]
- 438. Security Switch SNMP User Lookup [<index>]
- 439. STP Msti Port Cost [<msti>] [<stp_port_list>] [<path_cost>]
- 440. Security Switch SNMP Group Add <security_model> <security_name> <group_name>
- 441. STP Msti Port Priority [<msti>] [<stp_port_list>] [<priority>]
- 442. Security Switch SNMP Group Delete <index>
- 443. Security Switch SNMP Group Lookup [<index>]
- 444. Security Switch SNMP View Add <view_name> [included|excluded] <oid_subtree>
- 445. Security Switch SNMP View Delete <index>
- 446. Security Switch SNMP View Lookup [<index>]
- 447. Security Switch SNMP Access Add <group_name> <security_model> <security_level>
- [<read_view_name>] [<write_view_name>]
- 448. Security Switch SNMP Access Delete <index>
- 449. Security Switch SNMP Access Lookup [<index>]
- 450. Security Switch HTTPS Certificate Generate [rsa|dsa]
- 451. Security Switch HTTPS Certificate Load <hostname> <file_name>
- 452. Security Switch HTTPS Certificate Show
- 453. System Load
- 454. Security Network DHCP Snooping Configuration
- 455. Security Network DHCP Snooping Mode [enable|disable]
- 456. Security Network DHCP Snooping Port Mode [<port_list>] [trusted|untrusted]
- 457. Security Network DHCP Snooping Statistics [<port_list>] [clear]
- 458. [SIR \(Static IP Routing\) commands – see the related manual](#)

T

- 459. Thermal prio_temp [<prio_list>] [<shut_down_temp>]
- 460. Thermal port_prio [<port_list>] [<prio>]
- 461. Thermal status
- 462. Thermal configuration

U

- 463. Up

V

- 464. VCL Macvlan Configuration
- 465. VLAN Configuration [<port_list>]
- 466. VLAN Translation Add <group_id> <vid> <trans_vid>
- 467. VCL Macvlan Add <mac_addr> <vid> [<port_list>]
- 468. VLAN PVID [<port_list>] [<vid>|none]
- 469. VLAN Translation Delete <group_id> <vid>
- 470. VCL Macvlan Del <mac_addr>
- 471. VLAN FrameType [<port_list>] [all|tagged|untagged]
- 472. VLAN Translation Group [<port_list>] [<group_id>]
- 473. VCL Status [combined|static|nas|all]
- 474. VLAN IngressFilter [<port_list>] [enable|disable]
- 475. VLAN tx_tag [<port_list>] [untag_pvid|untag_all|tag_all]
- 476. VLAN PortType [<port_list>] [unaware|c-port|s-port|s-custom-port]
- 477. VLAN MPort PortType [unaware|c-port|s-port|s-custom-port]
- 478. VLAN remove <vid>|<name> [<port_list>]
- 479. VLAN EtypeCustomSport [<etype>]
- 480. VLAN Add <vid>|<name> [<ports_list>]
- 481. VLAN Forbidden Add <vid>|<name> [<port_list>]
- 482. VLAN Delete <vid>|<name>
- 483. VLAN Forbidden Delete <vid>|<name>
- 484. VLAN Forbidden Lookup [<vid>] [(name <name>)]
- 485. VLAN Lookup [<vid>] [(name <name>)] [combined|static|nas|mvr|evc|all]
- 486. VLAN Name Add <name> <vid>
- 487. VLAN Name Delete <name>
- 488. VLAN Name Lookup [<name>]
- 489. VLAN Status [<port_list>] [combined|static|nas|mvr|mstp|erps|mep|vcl|all|conflicts]
- 490. VCL ProtoVlan Protocol Add Eth2 <ether_type>|arp|ip|ipx|at <group_id>
- 491. VCL ProtoVlan Protocol Add Snap <oui>|rfc_1042|snap_8021h <pid> <group_id>
- 492. VCL ProtoVlan Protocol Add Llc <dsap> <ssap> <group_id>
- 493. VCL ProtoVlan Protocol Delete Eth2 <ether_type>|arp|ip|ipx|at
- 494. VCL ProtoVlan Protocol Delete Snap <oui>|rfc_1042|snap_8021h <pid>
- 495. VCL ProtoVlan Protocol Delete Llc <dsap> <ssap>
- 496. VCL ProtoVlan Vlan Add [<port_list>] <group_id> <vid>
- 497. VCL ProtoVlan Vlan Delete [<port_list>] <group_id>
- 498. VCL ProtoVlan Conf
- 499. VCL IPVlan Configuration [<vce_id>]
- 500. VCL IPVlan Add [<vce_id>] <ip_addr_mask> <vid> [<port_list>]
- 501. VCL IPVlan Delete <vce_id>

S3280 CLI Commands with Privilege Levels

Level 15 Commands	Levels 10-14	Levels 5-9	Levels 1-4
Aggr Add	X		
Aggr Configuration	X	X	
Aggr Delete	X		
Aggr Lookup	X	X	
Aggr Mode	X	X	
Config Backup Binary	X		
Config Default	X		
Config Restore Binary	X		
EPS command	X	X	
EPS config	X	X	
EPS create	X	X	
EPS state	X	X	
EVC Add	X	X	
EVC Configuration	X	X	
EVC Delete	X	X	
EVC ECE Add	X	X	
EVC ECE Delete	X	X	
EVC ECE Lookup	X	X	
EVC ECE Status	X	X	
EVC Lookup	X	X	
EVC Policer	X	X	
EVC Port Addr	X	X	
EVC Port DEI	X	X	
EVC Port L2CP	X	X	
EVC Port Tag	X	X	
EVC Statistics	X	X	
EVC Status	X	X	
Erps add	X		
Erps command	X		
Erps configuration	X	X	
Erps delete	X		
Erps guard	X		
Erps holdoff	X		
Erps mep	X		
Erps reversion	X		
Erps rpl neighbour	X		
Erps rpl neighbour clear	X		
Erps rpl owner	X		
Erps rpl owner clear	X		
Erps topologychange	X		
Erps version	X		
Erps vlan add	X		
Erps vlan delete	X		
Erps wtr	X		
EtherSAT commands – see related manual			

Level 15 Commands	Levels 10-14	Levels 5-9	Levels 1-4
Firmware IPv6 Load	X		
Firmware Information	X		
Firmware Load	X		
Firmware Swap	X		
Firmware Peripheral Versions	X		
Firmware Peripheral Load	X		
Help	X	X	X
IP ARP Show	X	X	
IP Configuration	X	X	
IP DHCP	X	X	
IP DNS	X	X	
IP DNS_Proxy	X	X	
IP IPv6 AUTOCONFIG	X	X	
IP IPv6 Ping6	X		
IP IPv6 Setup	X		
IP IPv6 State	X		
IP Mvlan	X		
IP NTP Configuration	X	X	
IP NTP Mode	X	X	
IP NTP Server Add	X		
IP NTP Server Delete	X		
IP NTP Server Ipv6 Add	X		
IP Ping	X		
IP Setup	X		
IPMC Compatibility	X	X	
IPMC Configuration	X	X	
IPMC Fastleave	X	X	
IPMC Filtering	X	X	
IPMC Flooding	X	X	
IPMC Groups	X	X	
IPMC Leave Proxy	X	X	
IPMC Mode	X	X	
IPMC Parameter LLQI	X	X	
IPMC Parameter QI	X	X	
IPMC Parameter QRI	X	X	
IPMC Parameter RV	X	X	
IPMC Parameter URI	X	X	
IPMC Proxy	X	X	
IPMC Querier	X	X	
IPMC Router	X	X	
IPMC SFM	X	X	
IPMC SSM	X	X	
IPMC State	X	X	
IPMC Status	X	X	
IPMC Throttling	X	X	
IPMC VLAN Add	X	X	
IPMC VLAN Delete	X	X	
IPMC Version	X	X	

Level 15 Commands	Levels 10-14	Levels 5-9	Levels 1-4
LACP Configuration	X	X	
LACP Key	X	X	
LACP Mode	X	X	
LACP Role	X	X	
LACP Statistics	X	X	
LACP Status	X	X	
LACP Timeout	X	X	
LACP Prio	X	X	
LACP System Prio	X	X	
LLDP Configuration	X	X	
LLDP Delay	X	X	
LLDP Hold	X	X	
LLDP Info	X	X	
LLDP Interval	X	X	
LLDP Mode	X	X	
LLDP Optional_TLV	X	X	
LLDP Reinit	X	X	
LLDP Statistics	X	X	
LLDP cdp_aware	X	X	
LOAM Control	X	X	
LOAM Frame_error_event	X		
LOAM Frame_error_seconds_summary_event	X		
LOAM Link_monitor_status	X	X	
LOAM Link_monitoring_support	X	X	
LOAM Mib	X	X	
LOAM Mode	X	X	
LOAM Remote_loopback_oper	X	X	
LOAM Remote_loopback_support	X	X	
LOAM Statistics	X	X	
LOAM Status	X	X	
LOAM Symbol_period_error_event	X		
LOAM Variable	X	X	
Logout	X	X	X
Loop Protect Configuration	X	X	
Loop Protect Mode	X	X	
Loop Protect Port Action	X	X	
Loop Protect Port Configuration	X	X	
Loop Protect Port Mode	X	X	
Loop Protect Port Transmit	X	X	
Loop Protect Shutdown	X	X	
Loop Protect Status	X	X	
Loop Protect Transmit	X	X	
MAC Add	X		
MAC Agetime	X	X	
MAC Configuration	X	X	
MAC Delete	X		
MAC Dump	X	X	
MAC Flush	X		

Level 15 Commands	Levels 10-14	Levels 5-9	Levels 1-4
MAC Learning	X	X	
MAC Lookup	X	X	
MAC Statistics	X	X	
MEP ais config	X	X	
MEP aps config	X	X	
MEP cc config	X	X	
MEP client config	X	X	
MEP config	X	X	
MEP dm clear	X	X	
MEP dm config	X	X	
MEP dm state	X	X	
MEP lb config	X	X	
MEP lb state	X	X	
MEP lck config	X	X	
MEP lm clear	X	X	
MEP lm config	X	X	
MEP lm state	X	X	
MEP lt config	X	X	
MEP lt state	X	X	
MEP peer MEP	X	X	
MEP state	X	X	
MEP tst clear	X	X	
MEP tst config	X	X	
MEP tst state	X	X	
MVR Configuration	X	X	
MVR Groups	X	X	
MVR Immediate Leave	X	X	
MVR Mode	X	X	
MVR SFM	X	X	
MVR Status	X	X	
MVR VLAN Channel	X	X	
MVR VLAN LLQI	X	X	
MVR VLAN Mode	X	X	
MVR VLAN Port	X	X	
MVR VLAN Priority	X	X	
MVR VLAN Setup	X	X	
Mirror Configuration	X	X	
Mirror Mode	X	X	
Mirror Port	X	X	
PTP ClockCreate	X	X	
PTP ClockDelete	X	X	
PTP Configuration	X	X	
PTP CurrentDS	X	X	
PTP DefaultDS	X	X	
PTP EgressLatency	X	X	
PTP Filter	X	X	
PTP ForeignMasters	X	X	
PTP LocalClock	X	X	

Level 15 Commands	Levels 10-14	Levels 5-9	Levels 1-4
PTP MasterTableUnicast	X	X	
PTP ParentDS	X	X	
PTP PortDataSet	X	X	
PTP PortState	X	X	
PTP Servo	X	X	
PTP SlaveTableUnicast	X	X	
PTP Timingproperties	X	X	
PTP UniConfig	X	X	
PTP ExtClock Output Mode	X	X	
PTP ExtClock Input Mode	X	X	
PTP ExtClock Impedance	X	X	
PTP ExtClock Input Status	X	X	
PTP Wireless mode	X	X	
PTP Wireless pre notification	X	X	
PTP Wireless delay	X	X	
PVLAN Add	X		
PVLAN Configuration	X	X	
PVLAN Delete	X		
PVLAN Isolate	X	X	
PVLAN Lookup	X	X	
Port Configuration	X	X	X
Port DMI Configuration	X	X	
Port DMI Statistics	X	X	X
Port Excessive	X	X	
Port Flow Control	X	X	
Port MaxFrame	X	X	
Port Mode	X	X	
Port Power	X	X	
Port SFP	X	X	X
Port State	X	X	
Port Statistics	X	X	X
Port VeriPHY	X		
QoS Configuration	X	X	
QoS DSCP Classification Map	X	X	
QoS DSCP Classification Mode	X	X	
QoS DSCP EgressRemap	X	X	
QoS DSCP Map	X	X	
QoS DSCP Translation	X	X	
QoS DSCP Trust	X	X	
QoS Port Classification Class	X	X	
QoS Port Classification DEI	X	X	
QoS Port Classification DPL	X	X	
QoS Port Classification DSCP	X	X	
QoS Port Classification Map	X	X	
QoS Port Classification PCP	X	X	
QoS Port Classification Tag	X	X	
QoS Port DSCP Classification	X	X	
QoS Port DSCP EgressRemark	X	X	

Level 15 Commands	Levels 10-14	Levels 5-9	Levels 1-4
QoS Port DSCP Translation	X	X	
QoS Port Policer FlowControl	X	X	
QoS Port Policer Mode	X	X	
QoS Port Policer Rate	X	X	
QoS Port Policer Unit	X	X	
QoS Port QueuePolicer Mode	X	X	
QoS Port QueuePolicer Rate	X	X	
QoS Port QueueShaper Excess	X	X	
QoS Port QueueShaper Mode	X	X	
QoS Port QueueShaper Rate	X	X	
QoS Port Scheduler Mode	X	X	
QoS Port Scheduler Weight	X	X	
QoS Port Shaper Mode	X	X	
QoS Port Shaper Rate	X	X	
QoS Port TagRemarking DEI	X	X	
QoS Port TagRemarking Map	X	X	
QoS Port TagRemarking Mode	X	X	
QoS Port TagRemarking PCP	X	X	
QoS QCL Add	X		
QoS QCL Delete	X		
QoS QCL Lookup	X	X	
QoS QCL refresh	X	X	
QoS QCL status	X	X	
QoS Storm Broadcast	X	X	
QoS Storm Multicast	X	X	
QoS Storm Unicast	X	X	
STP CName	X	X	
STP Configuration	X	X	
STP FwdDelay	X	X	
STP MaxAge	X	X	
STP MaxHops	X	X	
STP Msti Add	X		
STP Msti Map	X	X	
STP Msti Port Configuration	X	X	
STP Msti Port Cost	X	X	
STP Msti Port Priority	X	X	
STP Msti Priority	X	X	
STP Port AutoEdge	X	X	
STP Port Configuration	X	X	
STP Port Edge	X	X	
STP Port Mcheck	X		
STP Port Mode	X	X	
STP Port P2P	X	X	
STP Port RestrictedRole	X	X	
STP Port RestrictedTcn	X	X	
STP Port Statistics	X	X	
STP Port bpduGuard	X	X	
STP Status	X	X	

Level 15 Commands	Levels 10-14	Levels 5-9	Levels 1-4
STP Txhold	X	X	
STP Version	X	X	
STP bpduFilter	X	X	
STP bpduGuard	X	X	
STP recovery	X	X	
Security AAA ACCT_RADIUS	X	X	
Security AAA Configuration	X	X	
Security AAA Deadtime	X	X	
Security AAA RADIUS	X	X	
Security AAA Statistics	X	X	
Security AAA TACACS	X	X	
Security AAA Timeout	X	X	
Security Network ACL Action	X	X	
Security Network ACL Add	X		
Security Network ACL Clear	X		
Security Network ACL Configuration	X	X	
Security Network ACL Delete	X		
Security Network ACL Lookup	X	X	
Security Network ACL Policy	X	X	
Security Network ACL Port State	X		
Security Network ACL Rate	X	X	
Security Network ACL Status	X	X	
Security Network ARP Inspection Configuration	X	X	
Security Network ARP Inspection Entry	X		
Security Network ARP Inspection Mode	X	X	
Security Network ARP Inspection Port Mode	X	X	
Security Network ARP Inspection Status	X	X	
Security Network ARP Inspection Translation	X	X	
Security Network DHCP Relay Configuration	X	X	
Security Network DHCP Relay Information Mode	X	X	
Security Network DHCP Relay Information Policy	X	X	
Security Network DHCP Relay Mode	X	X	
Security Network DHCP Relay Server	X	X	
Security Network DHCP Relay Statistics	X	X	
Security Network DHCP Snooping Configuration	X	X	
Security Network DHCP Snooping Mode	X	X	
Security Network DHCP Snooping Port Mode	X	X	
Security Network DHCP Snooping Statistics	X	X	
Security Network IP Source Guard Configuration	X	X	
Security Network IP Source Guard Entry	X		
Security Network IP Source Guard Mode	X	X	
Security Network IP Source Guard Port Mode	X	X	
Security Network IP Source Guard Status	X	X	
Security Network IP Source Guard Translation	X	X	

Level 15 Commands	Levels 10-14	Levels 5-9	Levels 1-4
Security Network IP Source Guard limit	X	X	
Security Network Limit Action	X	X	
Security Network Limit Agetime	X	X	
Security Network Limit Aging	X	X	
Security Network Limit Configuration	X	X	
Security Network Limit Limit	X	X	
Security Network Limit Mode	X	X	
Security Network Limit Port	X	X	
Security Network Limit Reopen	X		
Security Network NAS Agetime	X	X	
Security Network NAS Authenticate	X		
Security Network NAS Configuration	X	X	
Security Network NAS EapolTimeout	X	X	
Security Network NAS Guest_VLAN	X	X	
Security Network NAS Holdtime	X	X	
Security Network NAS Mode	X	X	
Security Network NAS RADIUS_QoS	X	X	
Security Network NAS RADIUS_VLAN	X	X	
Security Network NAS ReauthPeriod	X	X	
Security Network NAS Reauthentication	X	X	
Security Network NAS State	X	X	
Security Network NAS Statistics	X	X	
Security Network Psec Port	X	X	
Security Network Psec Switch	X	X	
Security Switch Access Add	X		
Security Switch Access Clear	X		
Security Switch Access Configuration	X	X	
Security Switch Access Delete	X		
Security Switch Access Ipv6 Add	X		
Security Switch Access Lookup	X	X	
Security Switch Access Mode	X	X	
Security Switch Access Statistics	X	X	
Security Switch Auth Configuration	X	X	
Security Switch Auth Method	X	X	
Security Switch HTTPS Certificate Generate	X		
Security Switch HTTPS Certificate Load	X		
Security Switch HTTPS Certificate Show	X	X	
Security Switch HTTPS Configuration	X	X	
Security Switch HTTPS Mode	X	X	
Security Switch HTTPS Redirect	X	X	
Security Switch Privilege Level Configuration	x		
Security Switch Privilege Level Current	x		
Security Switch Privilege Level Group	x		
Security Switch RMON Alarm Add	X		
Security Switch RMON Alarm Delete	X		
Security Switch RMON Alarm Lookup	X	X	
Security Switch RMON Event Add	X		
Security Switch RMON Event Delete	X		

Level 15 Commands	Levels 10-14	Levels 5-9	Levels 1-4
Security Switch RMON Event Lookup	X	X	
Security Switch RMON History Add	X		
Security Switch RMON History Delete	X		
Security Switch RMON History Lookup	X	X	
Security Switch RMON Statistics Add	X		
Security Switch RMON Statistics Delete	X		
Security Switch RMON Statistics Lookup	X	X	
Security Switch SNMP Access Add	X		
Security Switch SNMP Access Delete	X		
Security Switch SNMP Access Lookup	X	X	
Security Switch SNMP Community Add	X		
Security Switch SNMP Community Delete	X		
Security Switch SNMP Community Lookup	X	X	
Security Switch SNMP Configuration	X	X	
Security Switch SNMP Engine ID	X	X	
Security Switch SNMP Group Add	X		
Security Switch SNMP Group Delete	X		
Security Switch SNMP Group Lookup	X	X	
Security Switch SNMP Mode	X	X	
Security Switch SNMP Read Community	X	X	
Security Switch SNMP Trap Authentication Failure	X	X	
Security Switch SNMP Trap Community	X	X	
Security Switch SNMP Trap Destination	X	X	
Security Switch SNMP Trap IPv6 Destination	X	X	
Security Switch SNMP Trap Inform Mode	X	X	
Security Switch SNMP Trap Inform Retry Times	X	X	
Security Switch SNMP Trap Inform Timeout	X	X	
Security Switch SNMP Trap Link	X	X	
Security Switch SNMP Trap Mode	X	X	
Security Switch SNMP Trap Probe Security Engine ID	X	X	
Security Switch SNMP Trap Security Engine ID	X	X	
Security Switch SNMP Trap Security Name	X	X	
Security Switch SNMP Trap Version	X	X	
Security Switch SNMP User Add	X		
Security Switch SNMP User Changekey	X		
Security Switch SNMP User Delete	X		
Security Switch SNMP User Lookup	X	X	
Security Switch SNMP Version	X	X	
Security Switch SNMP View Add	X		
Security Switch SNMP View Delete	X		
Security Switch SNMP View Lookup	X	X	
Security Switch SNMP Write Community	X	X	
Security Switch SSH Configuration	X	X	
Security Switch SSH Mode	X	X	
Security Switch Users Add	X		

Level 15 Commands	Levels 10-14	Levels 5-9	Levels 1-4
Security Switch Users Configuration	X		
Security Switch Users Delete	x		
sFlow Configuration	X		
sFlow CounterPoller	X		
sFlow FlowSampler	X		
sFlow Receiver	X		
sFlow Statistics Receiver	X		
sFlow Statistics Samplers	X		
SIR commands – see the related manual			
System Configuration	X	X	X
System Contact	X	X	
System Date	X	X	
System Load	X		
System Location	X	X	
System Log Clear	X		
System Log Configuration	X	X	X
System Log Level	X	X	
System Log Lookup	X	X	X
System Log Server Address	X	X	
System Log Server Mode	X	X	
System Name	X	X	
System PowerSupply Active	X	X	
System Reboot	x		
System Timezone Configuration	X	X	
System Timezone Offset	X	X	
System Timezone Acronym	X	X	
System DST Configuration	X	X	
System DST Mode	X	X	
System DST start	X	X	
System DST end	X	X	
System DST Offset	X	X	
System Version	X	X	X
Thermal configuration	X	X	
Thermal port_prio	X	X	
Thermal prio_temp	X	X	
Thermal status	X	X	
Up	X	X	X
VCL IPvlan Add	X		
VCL IPvlan Configuration	X	X	
VCL IPvlan Delete	X		
VCL Macvlan Add	X		
VCL Macvlan Configuration	X		
VCL Macvlan Del	X	X	
VCL ProtoVlan Conf	X		
VCL ProtoVlan Protocol Add Eth2	X	X	
VCL ProtoVlan Protocol Add Llc	X		
VCL ProtoVlan Protocol Add Snap	X		
VCL ProtoVlan Protocol Delete Eth2	X		

Level 15 Commands	Levels 10-14	Levels 5-9	Levels 1-4
VCL ProtoVlan Protocol Delete Llc	X		
VCL ProtoVlan Protocol Delete Snap	X		
VCL ProtoVlan Vlan Add	X		
VCL ProtoVlan Vlan Delete	X		
VCL Status	X	X	
VLAN Add	X		
VLAN Configuration	X	X	
VLAN Delete	X		
VLAN EtypeCustomSport	X	X	
VLAN Forbidden Add	X		
VLAN Forbidden Delete	X		
VLAN Forbidden Lookup	X	X	
VLAN FrameType	X	X	
VLAN IngressFilter	X	X	
VLAN Lookup	X	X	
VLAN Name Add	X		
VLAN Name Delete	X		
VLAN Name Lookup	X	X	
VLAN PVID	X	X	
VLAN PortType	X	X	
VLAN Status	X	X	
VLAN Translation Add	X		
VLAN Translation Delete	X		
VLAN Translation Group	X	X	
VLAN tx_tag	X	X	

Index

1:1 switching.....	212	IP Commands	26
1+1 switching.....	212	IPMC commands	328
AAA commands.....	152	latching loopback	355
Accounting commands	152	Link Aggregation.....	175
ACL commands.....	125	LL commands	355
ActiPHY mode	40	LLDP Aggregation.....	185
Aggregation commands	175	login	9
Authentication commands	152	Loop Protection commands	321
Authorization commands.....	152	M Port commands.....	56
backup command	24	MAC commands	51
change user's password.....	77	max frame size command.....	39
change user's privilege level	77	Mirror commands	259
change user's user name	77	Multicast Listener Discovery (MLD)	328
COM port settings	9	password, change.....	77
Commands, Config Management	24	Port Aggregation	175
commands, General	11	Port Commands	35
Commands, System	14	Precision Time Protocol.....	271
Conventions, documentation.....	6	PTP commands	271
delete a user.....	78	PV LAN commands.....	73
DMI command	46	QCL commands	233
Documentation conventions	6	QoS commands	233
ECE commands	195	QoS Control List.....	233
Editing Commands	7	Quality of Service.....	233
enter command mode	9	reboot command.....	23
EPS commands.....	212	reset to defaults command	24
ERPS commands	298	restore command	25
error messages	356	RMON commands	90
Ethernet linear Protection Switching	212	sample Flow.....	344
Ethernet Protection Switching	212	set up COM port.....	9
Ethernet Ring Protection Switching.....	298	sFlow commands	344
Ethernet services.....	195	SNMP commands	97
EtherSAT commands	355	STP commands	159
EVC commands	195	Technical support.....	390
Firmware commands	261	terminal emulation program	9
Help	7	Thermal protection commands	192
help screen	9	user name	9
HyperTerminal.....	9	VeriPHY, port	44
Internet Group Management Protocol (IGMP)	328	VLAN commands	57



Transition Networks

10900 Red Circle Drive

Minnetonka, MN 55343 USA

Tel: 952-941-7600 or 1-800-526-9267

Fax: 952-941-2322

Copyright © 2011, 2012, 2013 Transition Networks

All rights reserved.

Printed in the U.S.A.

S3280 Family of Carrier Ethernet Network Interface Devices (NIDs) CLI Reference Guide, 33507 Rev. F