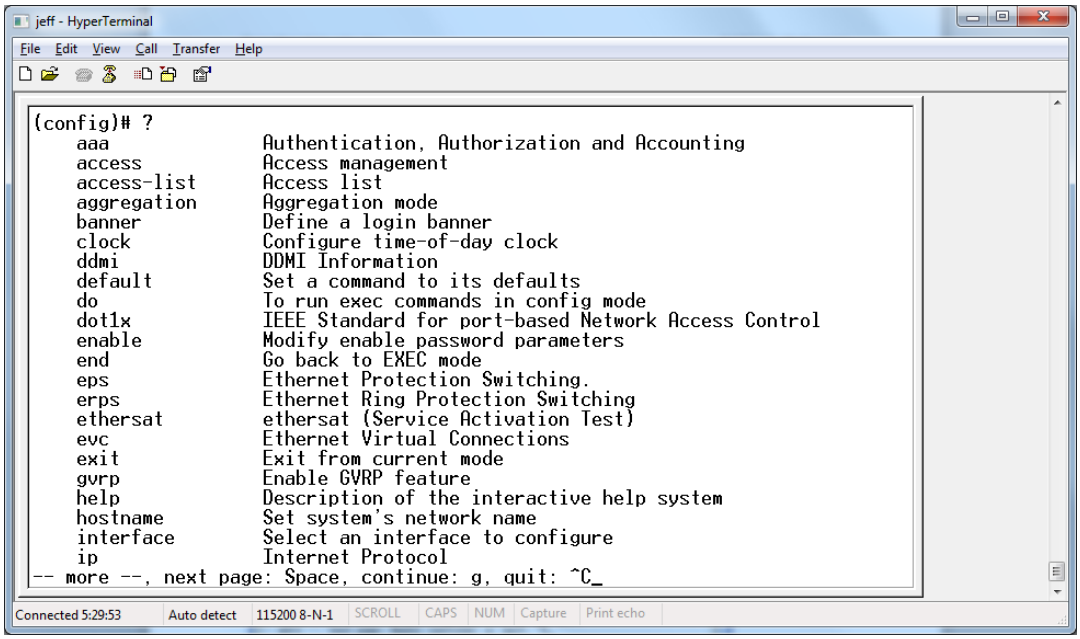
S4xxx CLI Reference



33559 Rev. B

Trademarks

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

Copyright Notice/Restrictions

S4140, S4212 & S4224 CLI Reference, 33555 Rev. B

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	12/11/14	Initial release for software v 2.0.x.
B	7/21/15	Updated to v 2.2 which adds GVRP, Service Activation Tests, DDMI, UDLD, PFC, and Perf- Mon support.

Cautions and Warnings

Definitions

Cautions indicate that there is the possibility of poor equipment performance or potential damage to the equipment. Warnings indicate that there is the possibility of injury to a person. Cautions and Warnings appear here and may appear throughout this manual where appropriate. Failure to read and understand the information identified by this symbol could result in poor equipment performance, damage to the equipment, or injury to persons. See the related Install Guide manual for specific Cautions and Warnings.

These products are not intended for use in life support products where failure of a product could reasonably be expected to result in death or personal injury. Anyone using this product in such an application without express written consent of an officer of Transition Networks does so at their own risk, and agrees to fully indemnify Transition Networks for any damages that may result from such use or sale.

Table of Contents

1 Introduction 8
1.1 Conventions 8
1.2 Starting a CLI Session 9
1.2.1 Login using HyperTerminal 9
1.2.2 Login using PuTTY 11
1.2.3 Login using Telnet 13
2 Quick Start 15
2.1 Log In and Reset Configuration to Factory Defaults 15
2.2 Set Device Hostname and admin User Password 16
2.3 Set VLAN 1 IP Address 16
2.4 Create Management VLAN and Set IP Address 17
2.5 Display and Save Configuration to FLASH 19
2.6 Summary 20
3 CLI Basics 21
3.1 Command Structure and Syntax 22
3.1.1 Command Syntax 23
3.2 Ethernet Interface Naming 25
3.3 Using the Keyboard 26
3.3.1 Basic Line Editing 26
3.3.2 Command History 27
3.3.3 Context-sensitive Help 28
3.3.4 Example: Context-sensitive Help 28
3.3.5 Long Lines and Pagination 29
3.3.6 Other Special Keys 30
3.4 Filtering Output 30
3.4.1 Example: Filtering Output 30
3.5 Understanding Modes and Sub-modes 31
3.5.1 Example: Using ‘do’ while in a Sub-mode 32
3.5.2 CLI Mode Transitions 33
3.5.3 Example: Changing between CLI Modes 33
3.6 Understanding Privilege Levels 34
3.6.1 Example: Configuring Privilege Level Passwords 34
3.7 Changing Terminal Session Parameters 35
4 Configuring the System 36
4.1 Configuration Example 36
4.2 Resetting or Removing Configuration Using ‘no’ Forms 37
4.3 Example: Using ‘no’ Forms 38
5 Add/Modify/Delete Users 39
5.1 Example: Add, Modify and Delete Users 39
6 Using ‘show’ Commands 40
6.1 Example: Listing All ‘show’ Commands 40
6.2 Example: Using Context-sensitive Help for Discovery 42
6.3 show running-config 43
6.3.1 Example: Default vs. Non-default vs. All Defaults 43
6.3.2 show running-config [all-defaults] 44
6.3.3 show running-config feature feature_name [all-defaults] 44
6.3.4 show running-config interface list [all-defaults] 45
6.3.5 show running-config vlan list [all-defaults] 45

6.3.6 show running-config interface vlan list [all-defaults] 45
6.3.7 show running-config line { console | vty } list [all-defaults] 45
7 Working with Configuration Files 46
7.1 Example: Working With Configuration Files 47
8 Working with Software Images 48
9 CLI Command Groups 49
show commands 50
config commands 51
copy commands 52
clear commands 52
Other EXEC commands 53
CLI Features and Modes 54
Global Configuration Mode List 55
VLAN Configuration Mode Example 56
Interface Configuration Mode Example 56
Privilege Levels 57
User EXEC Mode (> Prompt) 57
Privileged EXEC Mode (# Prompt) 57
Keyword Abbreviations 57
Error Checking 58
The “no” Form of Commands 58
Industry-standard Configuration Support 58
Sample running-config File 59
10 CLI Command Descriptions 63
CLI Command Groups 63
CLI Commands 63
? Help List of Commands 64
Command: ? 64
Clear (Reset) Commands 69
Command: Clear 69
Config Commands 71
Command: Configure Terminal Mode 71
Command: Configure AAA 72
Command: Configure Access Management 75
Command: Configure Access List ACE 76
Command: Configure Access List Rate Limiter 80
Command: Configure Aggregation 81
Command: Configure Banner 82
Command: Configure ToD Clock 82
Command: Configure DDMI 83
Command: Configure Default Access List Rate Limiter 84
Command: Configure Do 84
Command: Configure Dot1x NAC 85
Command: Configure Password Parameters 87
Command: End Configuration Mode 87
Command: Configure EPS 88
EPS (Port Protection) Parameters 91
Command: Config ERPS 93
ERPS Parameters 97

Command: Configure EtherSAT (Service Activation Test) 98
Command: Configure EVC 106
Command: Configure EVC ECE 109
EVC Policer Parameters 114
Command: Enable GVRP Feature 118
Command: Configure GVRP Max VLANs 118
Command: Configure GVRP Time 119
Command: Configure Help 120
Command: Configure Hostname 121
Command: Configure an Interface's Duplex/Excessive/FC/MAC/Media/MTU/Speed 123
Command: Configure Interface Switch / Ports 124
Command: Configure Interface VLAN 125
Command: Configure a Specific Interface SNMP Host Traps 131
Command: Configure IPv4 136
Command: Configure IP ARP Inspection 137
S4224 DHCP Configuration 143
IP DHCP Configuration Commands 143
IP DHCP Show Commands 143
IP DHCP Pool Commands (optional) 144
Running Config Example 145
Command: Configure IP Domain Name 147
Command: Configure IGMP Snooping 153
Command: Configure IGMP SSM Range 154
Command: Configure IGMP Unknown Flooding 154
Command: Configure IP DNS (Domain Name System) Name Server 155
Command: Configure IP SSH 158
Command: Configure IPv6 Static Routes 162
IPv6 MLD Snooping Parameters 164
Command: Configure Line 167
Sample Syslog Events 172
Command: Configure MAC Addr 174
Command: Configure MEP CCM-TLV 188
Command: Configure MEP ID 203
Command: Configure MEP Performance Monitoring (PM) 206
Command: Configure PTP Filter 235
Command: Configure PTP Debug Log Mode 236
Command: Configure PTP Clock Slave 243
Command: Configure PTP Time Properties 244
Command: QoS QCE Update 259
Command: Configure QoS Storm Policer 261
Related RMON RFCs 269
Command: Configure SNMP Server Contact Info 274
Command: Configure SNMP Server Host 275
Command: Configure SNMP Server Location 276
Command: Configure SNMP Server Security 276
Command: Configure SNMP Server Trap 277
Command: Configure SNMP Server MIB View 280
Command: Configure Spanning Tree 281
Command: Configure Username Authentication 290

VLAN Notes 293
VLAN Quick Config Example 294
Command: Configure Web Privilege Levels 295
Command: Copy Config File 297
Delete Commands 298
Command: Delete a File 298
Dir Commands 298
Command: Display Directory 298
Command: Disable Priviliged Command Mode 299
Command: Do (Run Exec Mode Command in Config Mode) 300
Command: Initialize 802.1x Interface 301
Command: Enable Priv Command Mode 303
Command: Exit EXEC mode 304
Command: Firmware Swap 305
Command: Firmware Upgrade 306
CLI Commands to Regain Access to the Web GUI 307
Help Commands 307
Command: Help 307
Command: IP v4 DHCP Command 308
Command: IP v6 DHCP Command 309
Command: Link OAM Remote Loopback Config 310
Command: Logout (Exit EXEC mode) 311
More (Display) Commands 311
Command: more 311
Command: No (Negate a Command or Set its Defaults) 312
Command: ping 315
PTP Commands 316
Reload Commands 317
Command: reload 317
Command: Send a Message 318
Command: Show Login Methods (AAA) 320
Command: Show Access Management Config 322
Command: Show Aggregation Port Configuration 327
Command: Show DDMI State 328
EPS Parameters 331
ERPS Parameters 334
Command: Show Internet Protocol (IP) Configs 348
Command: Show TTY Line Information 356
Command: Show LLDP and LLDP Med Info 358
MEP Basic Configuration Parameters 373
Command: Show NTP (Network Timing Protocol) Config 377
Platform-specific Parameters 380
PTP Parameters 389
PTP Servo Parameters 389
QCL and QCE Configuration 395
Command: Show RMON 397
Command: Show SNMP Config 403
Command: Show System CPU Status 413
Command: Show VLAN Information 420

Command: Set Terminal Parameters 424
Veriphy Commands 425
Command: Veriphy Interface 425
11 Messages 430
Service, Warranty & Compliance Information 430
Contact Us 431
Related Manuals and Online Help 431
Glossary 432

Figures

Figure 1. CLI Mode Transition Commands 33

Tables

Table 1. Basic Line Editing Keys 26
Table 2. Command History Keys 27
Table 3. Context-sensitive Help Keys 28
Table 4. Pagination Control Keys 29
Table 5. Other Special Keys 30
Table 6. Modes and Sub-modes 31

1 Introduction

This document describes the basic usage and configuration of the S4xxx (hereafter “S4224”) Command Line Interface (CLI).

The CLI is a fully comprehensive management interface on the device. It is the only management interface accessible on the serial console (i.e., even if there is no network connectivity, the device can still be managed using a serial connection).

Terminal input/output is shown below. User input (CLI command entry) is shown in **bold** font:

```
# show version

MEMORY : Total=86382 KBytes, Free=70497 KBytes, Max=70496 KBytes
FLASH : 0x40000000-0x40ffffff, 64 x 0x40000 blocks
MAC Address : 00-01-c1-00-ad-80
Previous Restart : Cold
...
```

1.1 Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen font`	Terminal sessions and information the system displays are in screen font.
`boldface screen` font	Information you must enter is in **boldface** screen font.
`italic screen` font	Arguments for which you supply values are in italic screen font.
!	This pointer highlights an important line of text in an example.
^	The caret symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters (such as passwords) are in angle brackets.
Note:	Indicates reader take note; contains helpful suggestions or references data not covered in this document.
Caution:	Means reader be careful. In this situation, you may do something that could result in equipment damage or loss of data.
Warning:	Means that you are in a situation that could cause bodily injury. Before you work on equipment, you must be aware of the hazards involved with electrical circuitry and be familiar with standard practices to prevent accidents.

1.2 Starting a CLI Session

The S4xxx (hreafter “S4224”) can be configured and managed directly or indirectly using:

HyperTerminal – offers a text-based command prompt on a remote device. The device could be a serial device, connected directly to your PC’s serial port or a network device. HyperTerminal can use the local serial interface for communications or the network for switch configuration and management.

PuTTY – a free Win32 Telnet and SSH client that can be used to access the CLI to configure and manage the switch via the network

Telnet session – uses the CLI to configure and manage the switch via the network.

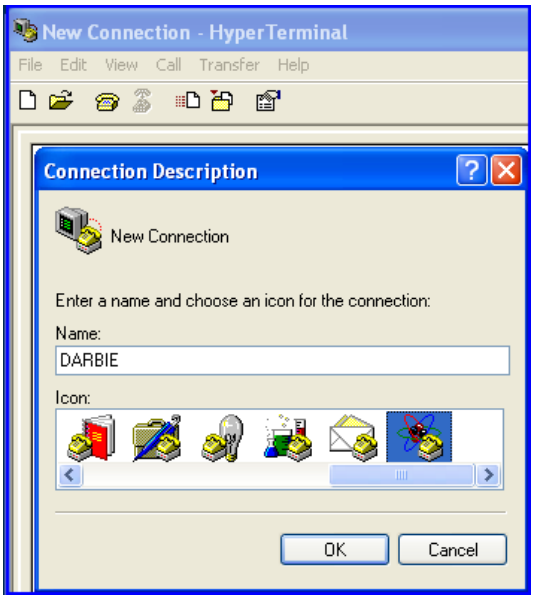
Web browser – uses any standard web browser and the IP address to access the S4224 web GUI for configuration and management.

SNMP (Simple Network Management Protocol) – uses public and private management information bases (MIBs) to easily integrate and manage the switch using a EMS (Element Management System).

The computer must be running a terminal emulator such as TeraTerm or PuTTY on Windows, or Minicom on Linux. Make a connection to a computer using the serial console port on the device (**115200** baud, **No** parity, **8** data bits, **1** stop bit, **no** flow control).

1.2.1 Login using HyperTerminal

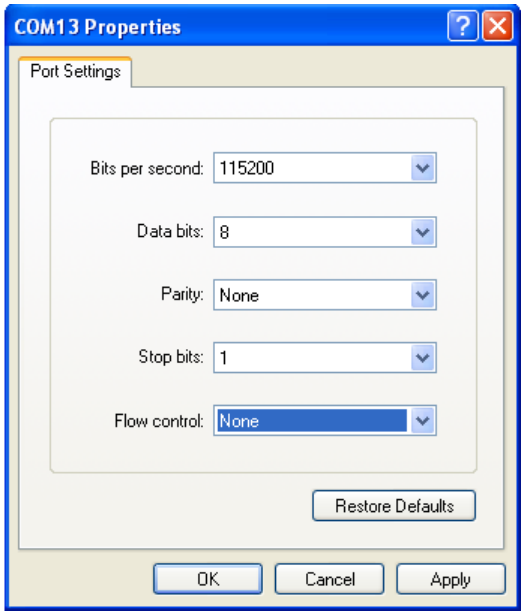
1. Connect the RJ-45 console cable from the S4224 to the computer.
2. On a Windows PC, go to START > Accessories > Communications > Hyper Terminal to bring up a New Connection - HyperTerminal screen.



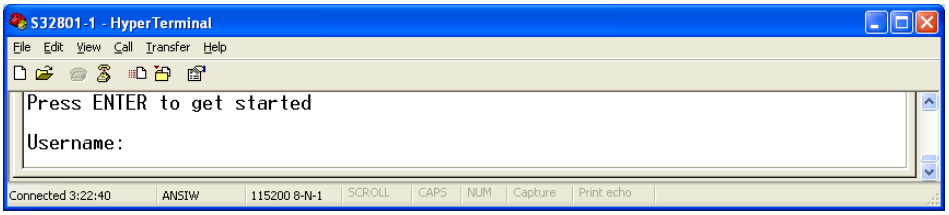
3. Type a name in the in the NAME field and select an Icon.

4. Click the OK to launch the “Connect To” dialog box. See the “Connect To” dialog box below.

5. Select a COM port on the “connect using” pulldown menu.
6. Click the **OK** button and the selected “COM Port Properties” dialog box appears, as shown below.
7. Set the COM Properties as shown below.

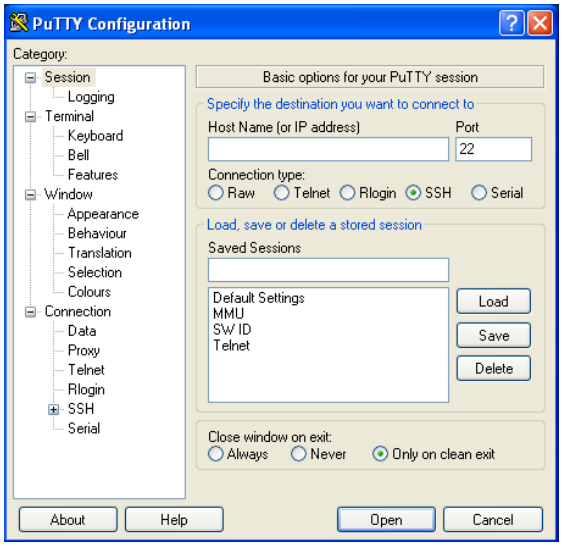


8. Click the **OK** button to establish the COM Port properties; the COM port dialog box will close.
9. Press the ENTER key twice to bring up the “username” prompt.
10. At the “username” prompt in lowercase type: admin, no password.
11. Press the ENTER key twice to launch the CLI interface (shown below).

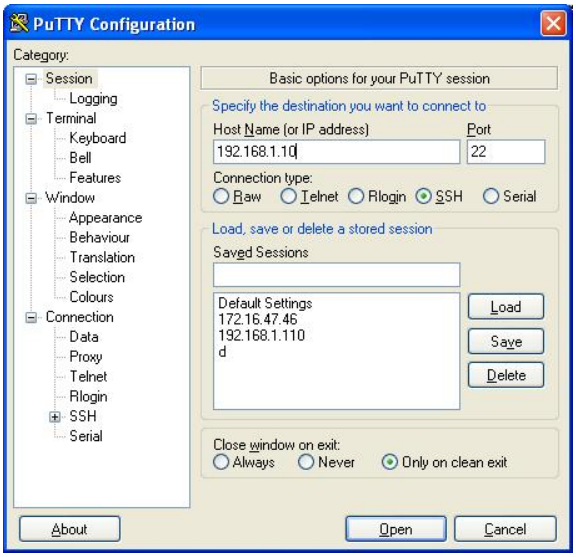


1.2.2 Login using PuTTY

1. Start a PuTTY session, and the PuTTY Configuration dialog box displays as shown below.



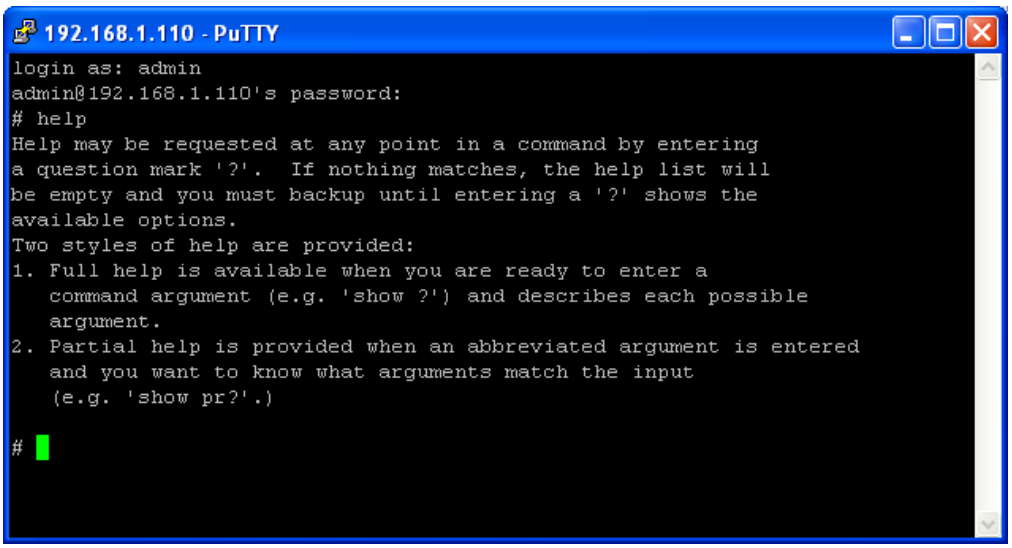
2. In the “Host Name {or IP Address}” field, enter the IP address of the switch (192.168.1.10).
3. In the Port field, enter 22.
4. Name the session in the “Saved Sessions” field.
5. Click the SAVE button and the dialog box displays as shown below.



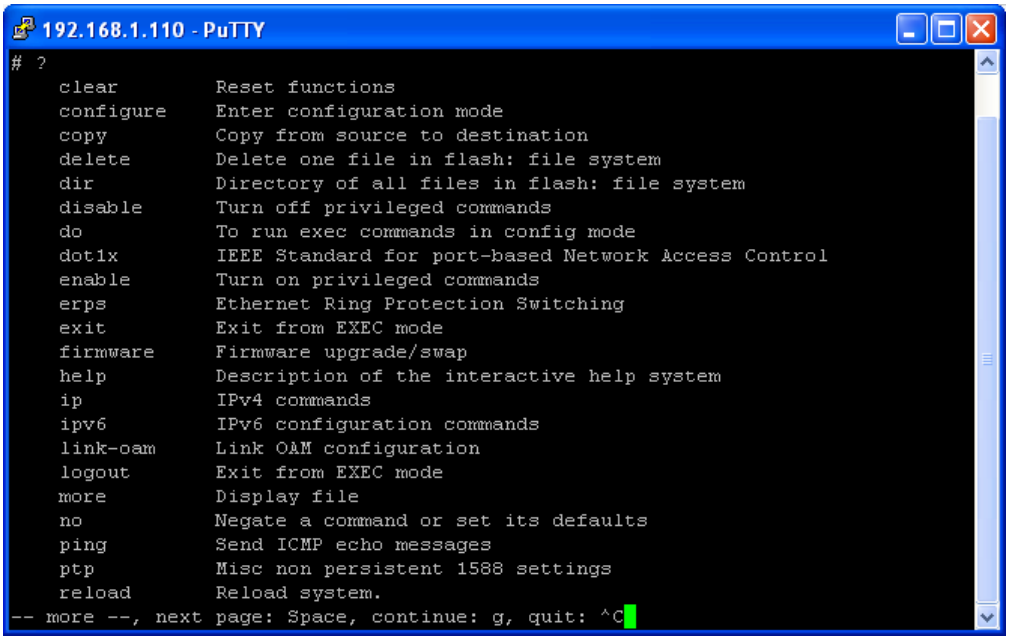
6. Click the **Open** button to launch the login screen, shown below. Note: If a Security Alert displays:
   - Click YES if you trust the host and the key will be added to the PuTTY cache.

- Click NO if you do not want to register the key for this session.

7. At the login prompt, type “admin” (default/lowercase).
8. Press the ENTER key three times to bring up the command prompt (see below).
9. Type “**help**” and press Enter to display the initial Help page as shown below.



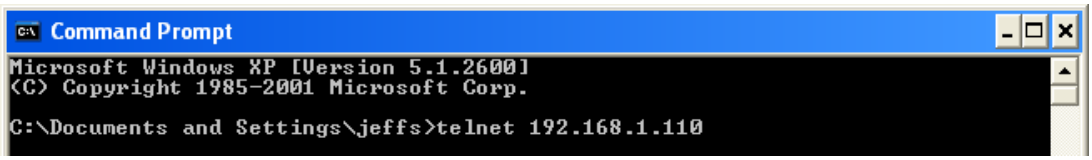
10. Type **?** display the initial commands list as shown below.



11. Continue as required; either press the Space bar to continue to the next page of the commands list or press Control - C (Ctrl/C) to quit and return to the # prompt.
12. See the command group descriptions or the Quick Start section below.

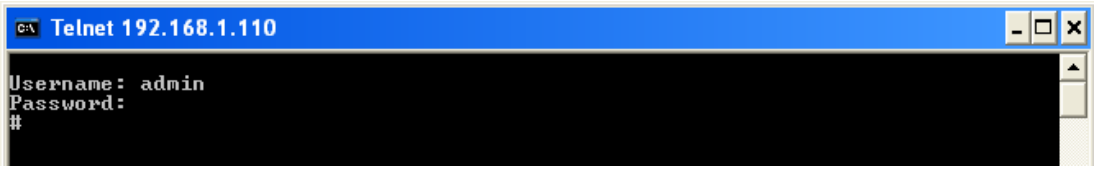
1.2.3 Login using Telnet

1. Using Windows, select START/Command Prompt.
2. At the prompt type **telnet** and then the S4224 IP address (e.g., **192.168.1.110** below).

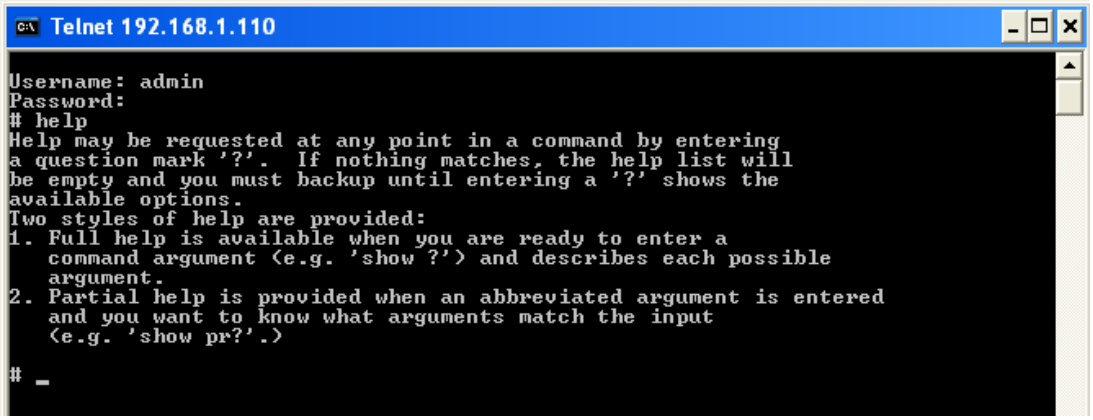


3. Click the **OK** button to launch the Telnet login screen, as shown below.

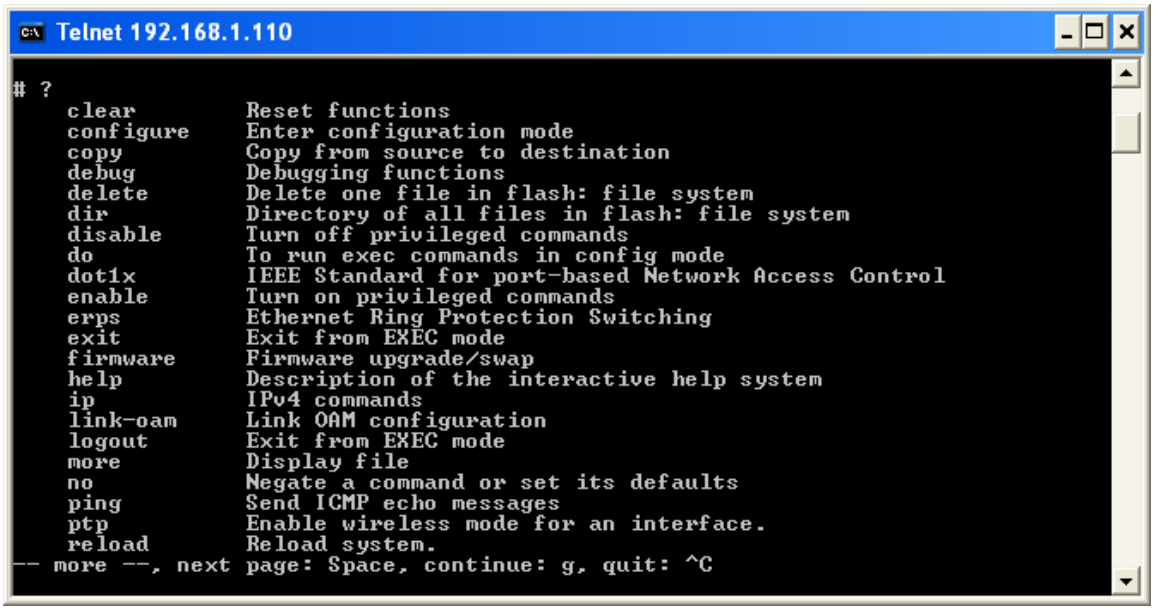
4. Enter the username "**admin**" (lowercase).
5. Press the ENTER key twice to bring up the # prompt as shown below.



6. Type "**help**" and press Enter to display the initial Help page as shown below.



7. Type **?** display the initial commands list as shown below.



8. Continue as required; either press the Space bar to continue to the next page of the commands list or press Control - C (Ctrl/C) to quit and return to the # prompt.
9. See the command group descriptions or the Quick Start section below.

2 Quick Start

This section is provided to help you quickly:

- Log in and reset configuration to factory defaults.
- Set device hostname and admin user password.
- Set VLAN 1 IP address.
- Configure a management VLAN and IP address and verify connectivity using ‘ping’.
- Display the current configuration and save it to FLASH storage.

The following assumes the device is powered on and has a functional connection to a computer using the serial console port on the device (**115200** baud, **No** parity, **8** data bits, **1** stop bit, **no** flow control).

The computer must be running a terminal emulator such as TeraTerm or PuTTY on Windows, or Minicom on Linux.

2.1 Log In and Reset Configuration to Factory Defaults

Press Enter one or more times until the ‘Username:’ prompt appears. Then type ‘admin’ and press the Enter key and at the ‘Password:’ prompt press Enter (there is no default password). This completes the login sequence and displays the prompt, ‘#’.

```
Username: admin
Password:
#
```

At this point the ‘admin’ user is operating at the highest privilege level, level 15. This means full control over the device and its configuration, and it is therefore possible to reset the configuration to factory defaults:

```
# reload defaults
% Reloading defaults. Please stand by.
# Reloading defaults complete.
#
```

When the prompt returns, the system has reverted to factory defaults.

Note: After power up, the S4224 has DHCP enabled. If a DHCP server is available, the S4224 will obtain an IP address from the DHCP server. If no DHCP server is available, after 70 seconds, the S4224 will fall back to the default IP address of 192.168.0.1/24.

2.2 Set Device Hostname and admin User Password

The CLI has several different modes. The current mode is called exec mode; it allows the user to perform operations related to configuration files, reloading defaults, displaying system information, etc., but it does not allow the user to change detailed configuration. Such operations are performed while in the configuration mode.

Thus, in order to set the device hostname, first change to configuration mode, then enter the 'hostname' command along with a suitable name, and finally 'exit' configuration mode:

```
# configure terminal
(config)# hostname my-device
my-device(config)# exit
my-device#
```

The commands are executed immediately, so 'hostname' changes the device hostname right away; this is reflected in the prompt as well.

A password should be set for the 'admin' user:

```
my-device# configure terminal
my-device(config)# username admin privilege 15 password unencrypted very-secret
my-device(config)# exit
my-device#
```

2.3 Set VLAN 1 IP Address

The objective is to assign an IP address to the device on VLAN 1, untagged. This is often sufficient for small networks, but not always recommended for operational or security reasons; the following section demonstrates a perhaps more secure approach.

The configuration proceeds in the same manner as setting the hostname: Enter configuration mode, input and execute configuration commands, leave configuration mode:

```
my-device# configure terminal
my-device(config)# interface vlan 1
my-device(config-if-vlan)# ip address 172.16.1.2 255.255.0.0
my-device(config-if-vlan)# exit
my-device(config)#
```

Notice how the prompt changes; the 'interface vlan 1' command enters a configuration *sub-mode* that allows, among other things, configuration of IP address.

Also note that IP addresses can only be assigned to VLAN interfaces.

The user 'admin' now has password 'very-secret'. Other users can be added in similar fashion, for more details see section 3.5.

2.4 Create Management VLAN and Set IP Address

The above approach has some potential weaknesses:

- All ports are by default members of VLAN 1, and
- the traffic is by default untagged.

This means that it is possible to manage the device from all ports, and that the management traffic isn't separated from other untagged traffic. If the switch is used in a trusted environment this may be acceptable; but if the network grows, it may become difficult to ensure authorized access to the device.

One way to address this is to use a *management VLAN* where all management traffic runs in a separate VLAN, and with a separate IP address space. This may or may not be sufficient in a real-world context; additional technical facilities exist but are beyond the scope of this document.

The objective is to use VLAN 42 as Management VLAN on interface GigabitEthernet 1 only, and the traffic on the VLAN must be tagged.

```
my-device# configure terminal
my-device(config)# interface vlan 1
my-device(config-if-vlan)# no ip address
my-device(config)# vlan 42
my-device(config-vlan)# name management
my-device(config-vlan)# interface vlan 42
my-device(config-if-vlan)# ip address 172.16.1.2 255.255.0.0
my-device(config-if-vlan)# interface GigabitEthernet 1/1
my-device(config-if)# switchport mode trunk
my-device# show vlan id 42
VLAN   Name                 Interfaces
----   --------------------------------       ----------
42     management           GigabitEthernet 1/1

my-device# show ip interface brief
Vlan   Address              Method       Status
----   --------------------       --------    ------
 42    172.16.1.2/16        Manual       UP
my-device#
```

First the IP address on interface vlan 1 is removed, and then VLAN 42 with the name 'management' is created, followed by the creation of an associated VLAN interface.

The VLAN is mainly a layer-2 entity whereas the VLAN interface is a layer-3 entity.

At this point the IP address is configured, followed by changing submode to interface configuration mode ('config-if') for GigabitEthernet 1/1. (**Note**: A port interface is named as 'type switch-id/port number'. Depending on hardware capabilities, the type may be FastEthernet or one of several GigabitEthernet variants such as 10GigabitEthernet. The switch ID indicates device index in a stacking setup; it is always 1 for systems that are not stacking capable.) The port can be in exactly one of three different modes; *access*, *trunk* and *hybrid*. A *trunk* port carries tagged VLANs and optionally untagged traffic assigned to a specific VLAN as well. By setting the port mode to 'trunk' we automatically include all VLANs (i.e., also VLAN 42).

The final two commands are used to verify settings:
First, ‘show vlan id 42’ displays information about VLAN 42: Name and the interfaces that are members, in this case exactly GigabitEthernet 1/1; the other interfaces on the device remain members of VLAN 1.
Second, ‘show ip interface brief’ displays configured and active IP interfaces. Note how the status should be ‘UP’.
If it isn’t, then the reason could be that there is no link on GigabitEthernet 1/1.

Now the most basic system configuration is complete. Management connectivity can be verified by issuing a ‘ping’ command to a well-known external IP address:

```
my-device# ping ip 172.16.1.1
PING server 172.16.1.1, 56 bytes of data.
64 bytes from 172.16.1.1: icmp_seq=0, time=0ms
64 bytes from 172.16.1.1: icmp_seq=1, time=0ms
64 bytes from 172.16.1.1: icmp_seq=2, time=0ms
64 bytes from 172.16.1.1: icmp_seq=3, time=0ms
64 bytes from 172.16.1.1: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
my-device#
```

If the ping is successful, network logins can now be performed via telnet or ssh to the address configured on VLAN interface 42, 172.16.1.2.

2.5 Display and Save Configuration to FLASH

The current configuration of the device can be displayed in the form of a virtual file containing the full set of commands necessary to create an identical configuration (with a few exceptions; certain items, such as private SSH keys, are not displayed.). This file is called ‘running-config’ and is ephemeral by nature; it does not survive across reboots. It is therefore necessary to save ‘running-config’ to FLASH storage under the name ‘startup-config’ – this file is read and is executed at every boot and is therefore responsible for restoring the running configuration of the system to the state it had when the last save occurred.

The ‘running-config’ is displayed with this command (note that some details were edited out for brevity, and the set of interfaces depends on hardware capabilities):

```
my-device# show running-config
Building configuration...
hostname my-device
username admin privilege 15 password encrypted dmVyeS1zZWNyZXQ=
!
vlan 1
 name default
!
vlan 42
 name management
!
spanning-tree mst name 00-01-c1-00-ad-80 revision 0
! [...]
!
interface GigabitEthernet 1/1
 switchport mode trunk
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
!
! [...]
!
interface 10GigabitEthernet 1/1
!
interface 10GigabitEthernet 1/2
!
interface vlan 1
 no ip address
!
interface vlan 42
 ip address 172.16.1.2 255.255.0.0
!
!
!
line console 0
!
line vty 0
!
! [...]
!
end
my-device#
```

Lines that begin with ‘!’ are comments. The file begins with the ‘hostname’ command and the password for user ‘admin’, and then followed by VLANs 1 and 42. Other configuration may display, such as Spanning Tree Protocol (STP).

Next, follows a list of all port interfaces on the device, ordered by switch ID, type and port number. All interfaces except GigabitEthernet 1/1 are at default settings, so nothing is displayed for them. This is a general rule of thumb: Only non-default configuration is displayed; otherwise the output would be huge and readability would suffer. There are exceptions, though, to be discussed later.

After the physical interfaces follows VLAN interfaces (1 and 42). Only the latter has an IP address assigned.

Finally, follows the 'line' section; it specifies characteristics for the serial console ('line console 0') or network CLI management connections ('line vty x').

The configuration as displayed above is also what is saved to 'startup-config':

```
my-device# copy running-config startup-config
Building configuration...
% Saving 1326 bytes to flash:startup-config

my-device# dir
Directory of flash:
 r- 1970-01-01 00:00:00 648 default-config
 rw 1970-01-03 18:21:28 1326 startup-config
2 files, 1974 bytes total.

my-device# more flash:startup-config
hostname my-device
username admin privilege 15 password encrypted dmVyeS1zZWNyZXQ=
!
vlan 1
 name default
[...]
```

The 'dir' command lists the files in the FLASH file system; the 'more' command outputs the contents of one of them.

2.6 Summary

This concludes the Quick Start. The skills exercised here form the basis for all day-to-day work with the Command Line Interface on the device: Logging in, displaying information ('show'), working with the configuration files ('show running-config', 'copy', 'dir', 'more'), working with the actual configuration ('configure terminal', 'exit') and submodes ('interface ...').

3 CLI Basics

The CLI has some key characteristics:

- The command prompt always displays the current mode.
- CLI commands are not *case-sensitive*.
- The CLI is *modal* (i.e., certain operations are possible or impossible in specific modes).
- It is *line-based* (i.e., no screen editing features).
- It executes commands instantly upon end-of-line.
- It is *privilege-based* (i.e., certain operations require the user to have a certain *privilege level* to succeed).
- It implements industrial de-facto behavior for network equipment CLIs (i.e., it structurally and behaviorally resembles CLIs found on other equipment while still possessing unique characteristics in some areas).

The CLI can be accessed directly via the serial console, or over the network via telnet or ssh. In each case users must log in before CLI commands can be executed; this begins a session which lasts until log out.

Multiple sessions can co-exist at the same time, each providing separate environments: Logged-in user ID, privilege level, command history, mode and session settings. It is therefore perfectly possible for the same user to control several concurrent sessions; for example, one serial console session and one ssh session.

The user database is either local or provided by a RADIUS or TACACS+ server. In case of a local user database, passwords and privilege levels are maintained on the device.

3.1 Command Structure and Syntax

A *command* is a single line of text consisting of *keywords* and *parameters*; for example:

```
my-device# show vlan id 10
...
my-device# show vlan id 20
...
```

The keywords are ‘show’, ‘vlan’, and ‘id’; whereas 10 and 20 are parameters, something that could contain another value in another command invocation.

Keywords and certain parameters can be abbreviated as long as they are unambiguous. For example, the two commands below are identical:

```
my-device# show interface GigabitEthernet 1/5 capabilities
...
my-device# sh in g 1/5 c
...
```

This works because:

1. There are many keywords that begin with ‘s’ but only one that begins with ‘sh’.
2. There are several commands that begin with ‘show i’ but only one that begins with ‘show in’.
3. The ‘show interface’ command takes a port type as parameter. Depending on the hardware capabilities, the options are: FastEthernet, GigabitEthernet, 10GigabitEthernet, 5GigabitEthernet and 10GigabitEthernet. So, ‘g’ is a unique abbreviation for ‘GigabitEthernet’.
4. The ‘1/5’ identifies the interface as belonging to switch 1, port 5. This parameter cannot be abbreviated and must be written out in full.
5. The ‘show interface GigabitEthernet 1/5’ command can output different kinds of information: Capabilities, statistics, status, and several others. In this case ‘c’ is a unique abbreviation for ‘capabilities’.

With a bit of practice this allows for highly efficient keyboard entry, in particular when coupled with the context-sensitive help features of the CLI (see section 3.3.3, Context-sensitive Help).

3.1.1 Command Syntax

A command is described by its syntax. The syntax is represented in a slightly different manner in this documentation and in a CLI session. In this document, variable parameters are written in *italics*, whereas a CLI session will display such items surrounded by '<' and '>'.

For example:

```
show interface list { status | statistics | capabilities | switchport | veriphy }
```

and

```
show erps [ groups ] [ detail | statistics ]
```

The semantics are:

- **keywords** are written in bold.
- *parameters* are written in italics.
- [...] indicates an optional construct: It may or may not be present.
- { ... } indicates a grouping; the constructs within belong together somehow.
- '|' indicates a choice between two or more alternatives (e.g., **a** | **b** | **c** which reads as "a or b or c").

Thus, the first command syntax is simple: First 'show', then 'interface', then a list of interfaces, then exactly one of 'status', 'statistics', 'capabilities', 'switchport' and 'veriphy'.

The second command is a bit more complex: 'show' and 'erps' are mandatory, but then the remaining parameters and keywords are optional: You may enter group IDs; you may enter either 'statistics' or 'detail'. For example:

```
! Show short-form ERPS (Ethernet Ring Protection Switching) information for all
! instances:
my-device# show erps
...

! Show statistics for all instances:
my-device# show erps statistics
...

! Show details for all instances:
my-device# show erps detail
...

! But it is not allowed to show details and statistics at the same time:
my-device# show erps detail statistics

                            ^
% Invalid word detected at '^' marker.

! Show details for specific set of instances:
my-device# show erps 1-6 detail
...
```

There are some slightly more complex features of the syntax that center around sequences of optionals such as [**a**] [**b**] [**c**].

- Each of a, b, c may or may not be present, e.g. “a c” is valid, as is no input at all.
- Order is not important, e.g. “a c” and “c a” are equivalent.
- Each optional can be present exactly zero or one time (i.e., not repeated).

There are variations:

- Group of optionals of which at least one must be present: **{ [a] [b] [c] }*1**
- Group of optional where one or more has fixed position: **[a] {[b]} [c]**
    - This says that ‘b’ is optional, but if it is present then it must follow after ‘a’ (if ‘a’ is present) *and* it must come before ‘c’ (if ‘c’ is present).

For example, assume a command with this syntax:

```
a [b] [c] { d | e } {[f] [g]}*1
```

then valid input examples are:

- ‘a d f’, because ‘b’ and ‘c’ are optional, ‘d’ is picked instead of ‘e’, and ‘f’ is chosen as the mandatory optional.
- ‘a d f g’, because ‘b’ and ‘c’ are optional, ‘d’ is picked instead of ‘e’, and both ‘f’ and ‘g’ are chosen in the final group of optional.
- ‘a c b e g’, because the ‘b’ optional is omitted, ‘e’ is picked instead of ‘d’, and ‘g’ is chosen for the mandatory optional.

3.2 Ethernet Interface Naming

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

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

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

As you can see, this allows a single list to mix different types.

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

Some examples are:

- GigabitEthernet 1/5 for the single gigabit port number 5 on switch 1.
- GigabitEthernet 1/2,4,10-12 for gigabit ports 2, 4, 10, 11, 12 on switch 1.
- GigabitEthernet 1-3/2 for gigabit port 2 on switches 1, 2 and 3.

It is possible to *wildcard* the type and/or switch ID and/or ports to mean “all types”, “all switch IDs” and “all ports”, respectively. A wildcard is written with an asterisk ‘*****’ instead of type, switch ID or port, and some further abbreviations are possible:

- ‘*****’ means “all ports of all types on all switches”.
- type ‘*’ means “all ports of the specified type on all switches”.

Some examples to clarify: Assume a stack with two switches, switch ID 1 and 3. Each switch has nine gigabit ports and two 2.5 gigabit ports. Then:

- interface * (or: interface * * *)
  - All ports of all types on all switches: GigabitEthernet 1,3/1-9 10GigabitEthernet 1,3/1-2
- interface * 1/2
  - Switch 1, port number 2 of all types: GigabitEthernet 1/2 10GigabitEthernet 1/2
- interface * */2
  - All switches, all types, port number 2: GigabitEthernet 1,3/2 10GigabitEthernet 1,3/2
- interface GigabitEthernet 3/*
  - Switch 3, all gigabit ports: GigabitEthernet 3/1-9.
- interface 10GigabitEthernet * (or: interface 10GigabitEthernet */*)
  - All 2.5 gigabit ports on all switches: 10GigabitEthernet 1,3/1-2.

Wildcards will include the largest possible set of ports, but may output an error message if a specific switch ID or port number doesn’t exist.

For example, these sets are invalid:

- interface * 2/*
  - All ports of all types on switch 2 – which isn't a member of the stack.
- interface * */100
  - There is no port 100 of any type on any switch.
- interface GigabitEthernet */* 10GigabitEthernet 2/*
  - Again, switch 2 doesn't exist so the entire set is considered invalid.

Validity is determined per set of (type, switch ID, port) containing wildcards: The result for that set is valid if there is at least one port that matches the set. A list of sets is valid if all sets match at least one port each.

For example, this is valid: interface * */1,100 – and the result is port 1 of all types on all switches.

3.3 Using the Keyboard

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

- Basic line editing
- Command history
- Context-sensitive help
- Long lines and pagination

3.3.1 Basic Line Editing

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

Table 1. Basic Line Editing Keys

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

3.3.2 Command History

A session maintains a non-persistent command history of previously entered command lines. The history can be up to 32 lines long; once full, a new line will push the oldest entry out.

Table 2. Command History Keys

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

The number of lines to keep in the history for the current session is configurable:

```
my-device# terminal history size 32
```

The size is a value from 0 to 32; entering 0 disables the history entirely.

The current value is displayed as part of the output from ‘show terminal’:

```
my-device# show terminal
Line is con 0.
     * You are at this line now.
      Alive from Console.
      Default privileged level is 2.
      Command line editing is enabled
      Display EXEC banner is enabled.
      Display Day banner is enabled.
      Terminal width is 80.
                  length is 24.
                  history size is 32.
                  exec-timeout is 10 min 0 second.

      Current session privilege is 15.
      Elapsed time is 0 day 0 hour 6 min 20 sec.
      Idle time is 0 day 0 hour 0 min 0 sec.
```

It is possible to list the history:

```
my-device# show history
 show running-config
 copy running-config startup-config
 dir
 show history
my-device#
```

The list begins with the oldest entry at top (‘show running-config’).

3.3.3 Context-sensitive Help

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

Table 3. Context-sensitive Help Keys

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

The context-sensitive help only displays commands that are accessible at the current session privilege level (see section 3.6).

3.3.4 Example: Context-sensitive Help

```
! Show possible next input for a command that begins with 'show a':
my-device# show a?
 aaa Login methods
 access Access management
 access-list Access list
 aggregation Aggregation port configuration

! The same, but without descriptions:
my-device# show a<TAB>
aaa access access-list aggregation

! If the user enters another 'g' the word 'aggregation' is the only possibility:
my-device# show ag?
 aggregation Aggregation port configuration
 <cr>

! Pressing <TAB> now expands the word fully:
my-device# show aggregation

! Possible next input is displayed with a press of '?':
my-device# show aggregation ?
        |            Output modifiers
        mode   Traffic distribution mode
        <cr>

! The syntax is displayed with another press of '?':
my-device# show aggregation ?
show aggregation [ mode ]

! This shows that there is an optional 'mode' word (square brackets indicate an
option).

! Repeated presses of '?' toggles display between next possible input and syntax:
my-device# show aggregation ?
      |              Output modifiers
      mode     Traffic distribution mode
      <cr>
my-device# show aggregation ?
show aggregation [ mode ]
```

```
! Finally, the syntax display is also directly available with Ctrl-Q:
my-device# show aggregation ^Q
show aggregation [ mode ]
```

3.3.5 Long Lines and Pagination

A session has configuration that indicates the width of the terminal in characters and the height in lines. It uses these parameters to control handling of long input lines and to control pagination of multi-line output. For details about changing these parameters please refer to section 3.7.

Long lines come into play when a line is longer than the terminal width minus the prompt. In that case part of the line will be hidden from display, as indicated by '$' at the beginning and/or end of the visible part of the line.

For example:

```
my-device# $there is text to the left of what is visible here
my-device# there is text to the right of what is visible here$
my-device# $there is text at both ends of what is visible here$
```

The first line has scrolled left; the second line has scrolled right; the third line has been scrolled to the middle of a quite long line.

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

```
! [lines of text]
-- more --, next page: Space, continue: g, quit: ^C
```

The following keys control pagination:

Table 4. Pagination Control Keys

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

The terminal height can be configured for the current session using the 'terminal height lines' command. If lines = 0 is input, pagination is disabled.

```
my-device# terminal length 0
my-device# terminal length 25
```

3.3.6 Other Special Keys

One additional key is defined as a convenience to allow the immediate return from any sub-mode to exec mode (see the section 3.5 - Understanding Modes and Sub-modes).

Table 5. Other Special Keys

Key	Operation
Ctrl-Z	Return directly to Exec mode.

3.4 Filtering Output

The output from commands can in most cases be filtered. It is possible to limit the output to only those lines that match/trigger a specific substring. The available filtering is:

- Begin – display the first line that matches and all subsequent lines
- Include – display exactly those lines that match
- Exclude – display exactly those lines that do not match

The syntax is:

```
command '|' { begin | include | exclude } string
```

3.4.1 Example: Filtering Output

```
! Execute a command that generates some output; no filtering initially:
my-device# show users
Line is con 0.
 * You are at this line now.
 Connection is from Console.
 User name is admin.
 Privilege is 15.
 Elapsed time is 0 day 21 hour 52 min 50 sec.
 Idle time is 0 day 0 hour 0 min 0 sec.

! Filter to include specific word:
my-device# show users | include User
 User name is admin.

! Exclude all lines that contain '0' (zero)
my-device# show users | exclude 0
 * You are at this line now.
 Connection is from Console.
 User name is admin.
 Privilege is 15.

! Begin output when specific word is matched:
my-device# show users | begin Elapsed
 Elapsed time is 0 day 21 hour 53 min 29 sec.
 Idle time is 0 day 0 hour 0 min 0 sec.
```

A vertical bar (| - the "pipe" symbol) indicates that an output processing specification follows.

3.5 Understanding Modes and Sub-modes

The CLI implements a number of modes that control the available command set. The modes are further influenced by the privilege level of the user; some modes or commands are only accessible to administrators while others require no privileges beyond log in.

There are three major modes, Exec, Privileged Exec and Config; and under Config there exist a number of sub-modes. The sub-modes allow configuration of specific VLANs, Ethernet interfaces, etc.

Table 6. Modes and Sub-modes

Mode	Parent Mode	Description
Exec	--	Lowest-privileged mode; used for basic system monitoring. Generally does not allow modifications to the system. Command: **`disable`**
Privileged Exec	Exec	Privileged mode; allows configuration and other modifications to the system. Command: **`enable`**
Config	Priv. exec	Global configuration mode. Command: **`configure terminal`**
VLAN config	Config	Sub-mode for configuring active VLANs. Command: **`vlan vlan_id_list`**
VLAN interface config	Config	Sub-mode for configuring VLAN interfaces Command: **`interface vlan vlan_id_list`**
Interface config	Config	Sub-mode for configuring Ethernet interfaces Command: **`interface type switch_num/port_num`**
Line	Config	Sub-mode for configuring terminal lines. Command: **`line { con | vty } line_num`**
IPMC Profile Config	Config	Sub-mode for configuring IP Multicast profiles. Command: **`ipmc profile profile_name`**
SNMP Server Host Config	Config	Sub-mode for configuring SNMP server host entries. Command: **`snmp-server host host_name`**
STP Aggregation Config	Config	Sub-mode for configuring Spanning Tree Protocol aggregation Command: **`spanning-tree aggregation`**
DHCP Pool Config	Config	Sub-mode for configuring DHCP client pools. Command: **`ip dhcp pool pool_name`**
RFC2544 Profile Config	Config	Sub-mode for configuring RFC2544 profiles. Command: **`rfc2544 profile profile_name`**

It is possible for a user to transition between these modes using certain commands, subject to the user's privilege level and the current session privilege level (see section 3.6).

The initial mode is determined by the privilege level of the user logging in. If the privilege level is zero or one the user is *unprivileged* and begins in the (Unprivileged) Exec mode. If the privilege level is higher, then the session begins in Privileged Exec mode.

A user can raise the Exec mode privilege level to a higher value if an *enable password* has been configured for that level. This elevation is done with the 'enable level' command, where level is a value

between 1 and 15. The reverse operation, lowering the privilege level, is achieved with the ‘disable’ command.

Once in Privileged Exec mode it is possible to enter into the Global Configuration mode by entering the command ‘configure terminal’. Exit from Global Configuration is achieved with one of ‘end’, ‘exit’ or Ctrl-Z.

Access to a configuration sub-mode (e.g. for Ethernet interfaces) goes through Global Configuration or another sub-mode (i.e., it is possible to change directly from, say, VLAN sub-mode to Ethernet interface sub-mode).

Each mode and sub-mode thus implements a scope for commands: Inside each mode a particular subset of commands is available; to get to other commands one must generally change mode/sub-mode. This is necessary because there are commands with identical prefixes in different modes; for example there are commands that begin with ‘ip’ in Privileged Exec, Global Configuration and VLAN Interface Configuration modes.

There are two exceptions to this:

- While in a configuration sub-mode, access to Global Configuration mode commands is possible as long as there is no ambiguity. Execution of a Global Configuration command exits the sub-mode.
- Exec mode commands, be that privileged or unprivileged, are accessible from within Global Configuration or one of the sub-modes by using the ‘do’ command.

The ‘do’ command takes an arbitrary command line from Exec and executes it. In the following example, the user wants to change the IP address on the VLAN 1 interface, but wants to verify the current address while in the sub-mode.

3.5.1 Example: Using ‘do’ while in a Sub-mode

```
my-device# configure terminal
my-device(config)# interface vlan 1
my-device(config-if-vlan)# do show ip interface brief
Vlan Address Method Status
---- -------------------- -------- ------
 1 172.16.1.15/24 DHCP UP
my-device(config-if-vlan)# end

! When in Exec, no ‘do’ prefix is needed:
my-device# show ip interface brief
Vlan    Address                      Method  Status
----    -------------------  --------       ------
  1     172.16.1.15/24               DHCP           UP
```

3.5.2 CLI Mode Transitions

The figure below shows the possible transitions between major modes and sub-modes, and some of the related commands.

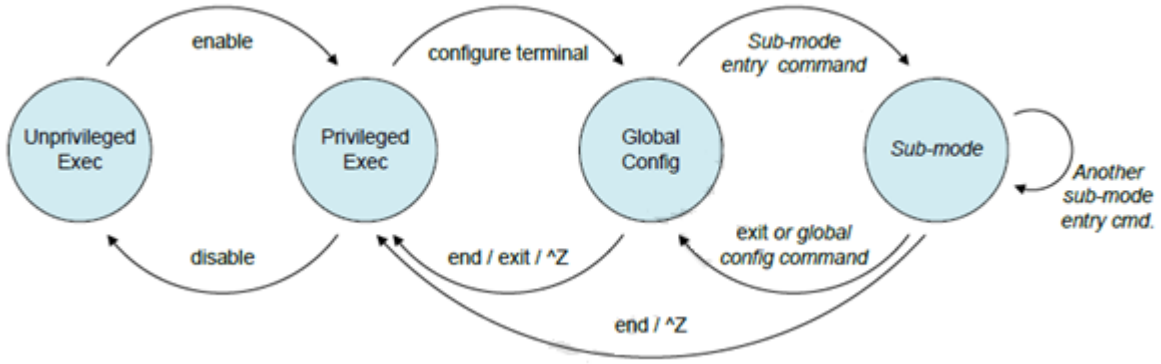


Figure 1. CLI Mode Transition Commands

3.5.3 Example: Changing between CLI Modes

```
! Initial mode for this example is Unprivileged Exec. Raise level
! (and change mode):
my-device> enable
Password: ***
my-device#

! Note how the prompt changed from '>' to '#' to indicate the privileged exec mode

! Enter Global Configuration mode:
my-device# configure terminal

! Now create VLAN 100 and give it a name. This enters the VLAN sub-mode, as
! indicated by a new prompt:
my-device(config)# vlan 100
my-device(config-vlan)# name MyVlan

! Change directly from VLAN sub-mode into Ethernet interface sub-mode for
! interface instance 4 on switch 1, and set link speed to 'auto'
my-device(config-vlan)# interface GigabitEthernet 1/4
my-device(config-if)# speed auto

! Then enter a command from the global configuration mode; this leaves Ethernet
! interface sub-mode
my-device(config-if)# hostname my-device

! Exit Global Configuration mode and go back to Privileged Exec
my-device(config)# end

! And use 'disable' to go back to Unprivileged Exec:
my-device# disable
my-device>
```

3.6 Understanding Privilege Levels

A *privilege level* is a number in the range 0 to 15, inclusive, with 0 being the lowest. It is assigned to a user session and used to determine access to CLI commands: Only commands at the same or lower privilege level can be accessed. Each user on the device has a default privilege level which is copied to the session's privilege level at log in. It is, however, possible for the user to change the session privilege level by executing the 'enable' or 'disable' commands. This can be used, for example, as follows:

- The user account is configured with privilege level 0.
- Whenever the user needs to perform higher-privileged commands, the user changes session priority level, executes the necessary commands, and then revert back to the default priority level.

Access to higher priority levels must be password protected by using the 'enable password' or 'enable secret' global configuration commands. The main difference between the two is whether passwords are displayed in clear text or encrypted form in running-config (and, consequently, startup-config).

Password input can also be in encrypted or clear text form. The latter is used when an operator input a new password, as the operator will usually not know the encrypted form of the password.

The 'admin' user is by default at level 15 (i.e., at the highest possible privilege level).

3.6.1 Example: Configuring Privilege Level Passwords

The following example configures a level 15 password using 'enable secret', inspects the resulting configuration, then removes it again.

```
my-device# configure terminal

! A secret can either be input in clear text or encrypted form; a digit indicates
! which kind follows on the command line:
my-device(config)# enable secret ?
      0 Specifies an UNENCRYPTED password will follow
      5 Specifies an ENCRYPTED secret will follow

! In this case: Unencrypted. Then follows either the level for which a password
! is being configured, or, if no level is given, the password for level 15:
my-device(config)# enable secret 0 ?
      <word32> Password
      level Set exec level password

! Thus, the following two commands are semantically identical:
my-device(config)# enable secret 0 my-secret
my-device(config)# enable secret 0 level 15 my-secret

! The running configuration can be inspected to see the encrypted form:
my-device(config)# do show running-config | include enable
enable secret 5 level 15 D29441BF847EA2DD5442EA9B1E40D4ED

! To remove the password use the 'no' form (the two are semantically equivalent
for level 15):
my-device(config)# no enable secret
my-device(config)# no enable secret level 15
my-device(config)# do show running-config | include enable
my-device(config)#
```

3.7 Changing Terminal Session Parameters

The CLI display terminal connection can be configured in terms of:

editing Enable command line editing.
exec-timeout Set the EXEC timeout (0-1440 minutes).
help Description of the interactive help system (full / partial help).
history Control the command history command storage size (0-32 commands).
length Set number of lines on a screen (0 for no pausing or 3-512 lines).
width Set width of the display terminal

The example below shows the command parameters and a sample show terminal command output.

```
# terminal editing
# terminal exec-timeout ?
    <0-1440>    Timeout in minutes
# terminal help
Help may be requested at any point in a command by entering a question mark '?'.  If nothing
matches, the help list will be empty and you must backup until entering a '?' shows the
available options. Two styles of help are provided:
1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and
describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what
arguments match the input (e.g. 'show pr?'.)
# terminal hist size ?
    <0-32>    Number of history commands, 0 means disable
# terminal length ?
    0 or 3-512    Number of lines on screen (0 for no pausing)
# terminal width ?
    0 or 40-512    Number of characters on a screen line (0 for unlimited width)
# show terminal ?
    |       Output modifiers
    <cr>
# show terminal
Line is con 0.
    * You are at this line now.
    Alive from Console.
    Default privileged level is 2.
    Command line editing is enabled
    Display EXEC banner is enabled.
    Display Day banner is enabled.
    Terminal width is 80.
             length is 24.
             history size is 32.
             exec-timeout is 10 min 0 second.

    Current session privilege is 15.
    Elapsed time is 0 day 0 hour 29 min 50 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

#
```

4 Configuring the System

Changes to the system configuration can only be done from the Global Configuration mode and its sub-modes (except when working with configuration files or reloading defaults; this is done in Privileged Exec mode).

The process is:

1. Raise privilege level to 15.
2. Enter Global Configuration mode.
3. Input appropriate configuration commands.
   a. Optionally enter sub-modes and input appropriate commands there.
4. Exit Global Configuration mode.
5. Verify configuration.
6. Save configuration to FLASH.

4.1 Configuration Example

In this example the hostname and VLAN 1 IP address is configured, verified and saved.

```
! This example assumes the session is initially unprivileged.

! Step 1: Raise privilege level:
> enable
Password: ***

! Step 2: Enter Global Configuration mode:
# configure terminal

 ! Step 3: Input configuration commands. The IP address is set from within the
! VLAN interface submode:
(config)# hostname my-device
my-device(config)# interface vlan 1
my-device(config-if-vlan)# ip address dhcp fallback 172.16.1.2 255.255.0.0
my-device(config-if-vlan)# exit

! Step 4: Leave Global Configuration mode and go back to Privileged Exec:
my-device(config)# end

! Step 5: Inspect and verify the configuration (some output omitted for brevity):
my-device# show running-config
Building configuration...
hostname my-device
username admin privilege 15 password encrypted Zm9v
!
vlan 1
 name default
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
...
interface vlan 1
 ip address dhcp fallback 172.16.1.2 255.255.0.0
!
```

```
...
end

! More verification: Display IP interfaces and assigned IP address and status:
my-device# show ip interface brief
Vlan Address Method Status
---- ------------------- -------- ------
 1 172.16.1.15/24 DHCP UP

! An address was obtained from DHCP, so the fallback wasn't used

! Try to inspect hostname:
my-device# show hostname
         ^
% Invalid word detected at '^' marker.

! No such command exists, but it is possible to extract a single line from
! running-config by using a filter:
my-device# show running-config | include hostname
hostname my-device

! Step 6: Save configuration to FLASH:
my-device# copy running-config startup-config
Building configuration...
% Saving 1272 bytes to flash:startup-config
```

4.2 Resetting or Removing Configuration Using 'no' Forms

It is possible to either remove specific configuration or reset it to its default values.

In the general case, almost each configuration command has a corresponding 'no' form. The 'no' form is syntactically similar (but not necessarily identical) to the configuration command, but either resets the parameters to defaults for the configurable item being addressed, or removes the item altogether.

In many cases 'no' can be read as "no(t) different from default settings".

4.3 Example: Using ‘no’ Forms

The following example:

- Configures the VLAN 1 interface IP address to use DHCP
- Configures the DNS name server to be taken from DHCP
- Inspects the configuration
- Removes the DNS name server
- Removes the IP address on the VLAN 1 interface

Both ‘no’ operations can be viewed as reset-to-default, with the defaults being: No DNS name server and IP address.

```
my-device# configure terminal
my-device(config)# interface vlan 1
my-device(config-if-vlan)# ip address dhcp
my-device(config-if-vlan)# exit
my-device(config)# ip name-server dhcp
my-device(config)# end

my-device# show ip interface brief
Vlan Address Method Status
---- -------------------- -------- ------
 1 172.16.1.15/24 DHCP UP

my-device# show ip name-server

Current DNS server is 172.16.1.1 set by DHCP.

my-device# configure terminal
my-device(config)# no ip name-server
my-device(config)# interface vlan 1
my-device(config-if-vlan)# no ip address
my-device(config-if-vlan)# end
my-device# show ip name-server

Current DNS server is not set.
my-device# show ip interface brief
Vlan Address Method Status
---- -------------------- -------- ------
my-device#
```

Note how the syntax of the configuration commands and their ‘no’ forms are different; the ‘no’ forms usually do not take as many parameters.

5 Add/Modify/Delete Users

This section describes local user management on the device. RADIUS and TACACS+ user management is beyond the scope of this document.

It is possible to create several user accounts on a system. Each user account has a set of configurable attributes:

- User name
- Password
- Privilege level

All attributes are configured with the same command, ‘username’.

```
username username privilege level password { unencrypted | encrypted } password
username username privilege level password none
no username username
```

Use ‘password none’ when no password is desired; the security implications of using this should be considered carefully.

Use ‘no username’ to delete the given user account.

5.1 Example: Add, Modify and Delete Users

The following example adds two user accounts at different privilege levels, inspects configuration, and deletes one account again using ‘no username’.

```
! Display current set of local user accounts:
my-device# show running-config | include username
username admin privilege 15 password encrypted dmVyeS1zZWNyZXQ=
! Add two accounts, ‘operator’ and ‘monitor’. The passwords are supplied in
! unencrypted form:
my-device# configure terminal
my-device(config)# username operator privilege 10 password unencrypted a-secret
my-device(config)# username monitor privilege 1 password unencrypted new-secret
! Verify that the configuration is correct. Note that passwords are displayed
! in encrypted form:
my-device(config)# do show running-config | include username
username admin privilege 15 password encrypted dmVyeS1zZWNyZXQ=
username operator privilege 10 password encrypted YS1zZWNyZXQ=
username monitor privilege 1 password encrypted YW5vdGhlci1zZWNyZXQ=

! Delete the ‘operator’ user and verify it is removed from the configuration:
my-device(config)# no username operator
my-device(config)# do show running-config | include username
username admin privilege 15 password encrypted dmVyeS1zZWNyZXQ=
username monitor privilege 1 password encrypted YW5vdGhlci1zZWNyZXQ=
```

6 Using ‘show’ Commands

The family of ‘show’ commands is the cornerstone of CLI-based system monitoring. Most features implement one or more ‘show’ commands that will display a relevant mix of status and configuration.

Note: The exact set of available commands, parameters and output format depends on the system configuration and software version, so some of the following commands and examples may not be applicable to all systems.

The ‘show’ commands exist only in the two Exec modes and are subject to session privilege level enforcement. Therefore, listing the largest possible set of ‘show’ commands requires the session to be at level 15.

6.1 Example: Listing All ‘show’ Commands

The following example raises the session privilege level to 15. In this example an ‘enable secret’ was specified, so password entry is required to proceed.

Then a ‘show’ command is entered, and the context-sensitive help feature is used to list the possible show commands (in this case for a Carrier Ethernet system).

```
Press ENTER to get started

Username: admin
Password:
# show ?
    aaa               Authentication, Authorization and Accounting methods
    access            Access management
    access-list       Access list
    aggregation       Aggregation port configuration
    clock             Configure time-of-day clock
    ddmi              DDMI configuration
    dot1x             IEEE Standard for port-based Network Access Control
    eps               Ethernet Protection Switching
    erps              Ethernet Ring Protection Switching
    ethersat          ethersat (Service Activation Test)
    evc               Ethernet Virtual Connections
    green-ethernet    Green ethernet (Power reduction)
    history           Display the session command history
    interface         Interface status and configuration
    ip                Internet Protocol
    ipmc              IPv4/IPv6 multicast configuration
    ipv6              IPv6 configuration commands
    lacp              LACP configuration/status
    line              TTY line information
    link-oam          Link OAM configuration
    lldp              Display LLDP neighbors information.
    logging           System logging message
    loop-protect      Loop protection configuration
    mac               Mac Address Table information
    mep               Maintenance Entity Point
```

```
    monitor           Monitoring different system events
    mvr               Multicast VLAN Registration configuration
    ntp               Configure NTP
    perf-mon          Performance Monitor
    platform          Platform configuration
    port-security     Port Security status - Port Security is a module with no
                      direct configuration.
    privilege         Display command privilege
    process           process
    ptp               Precision time Protocol (1588)
    pvlan             PVLAN configuration
    qos               Quality of Service
    radius-server     RADIUS configuration
    rmon              RMON statistics
    running-config    Show running system information
    snmp              Display SNMP configurations
    spanning-tree     STP Bridge
    switchport        Display switching mode characteristics
    system            system
    tacacs-server     TACACS+ configuration
    terminal          Display terminal configuration parameters
    udld              Uni Directional Link Detection(UDLD) configurations,
                      statistics and status
    user-privilege    Users privilege configuration
    users             Display information about terminal lines
    version           System hardware and software status
    vlan              VLAN status
    web               Web
# show
```

6.2 Example: Using Context-sensitive Help for Discovery

The context-sensitive help feature for syntax display is useful as well while drilling down on the exact command to execute. In the example below, the user discovers the proper command ‘show ip statistics system’ through exploration:

```
my-device# show ip ?
 arp Address Resolution Protocol
 dhcp Dynamic Host Configuration Protocol
 http Hypertext Transfer Protocol
 igmp Internet Group Management Protocol
 interface IP interface status and configuration
 name-server Domain Name System
 route Display the current ip routing table
 source source command
 ssh Secure Shell
 statistics Traffic statistics
 verify verify command

my-device# show ip statistics ?
 | Output modifiers
 icmp IPv4 ICMP traffic
 icmp-msg IPv4 ICMP traffic for designated message type
 interface Select an interface to configure
 system IPv4 system traffic
 <cr>

! A repeated press of ‘?’ displays the syntax:
my-device# show ip statistics ?
show ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ]
[ icmp-msg <type> ]

my-device# show ip statistics system

IPv4 statistics:

 Rcvd:  2768 total in 181458 bytes
        1727 local destination, 0 forwarding
        0 header error, 0 address error, 0 unknown protocol
        0 no route, 0 truncated, 0 discarded
 Sent:  2553 total in 180047 bytes
        1512 generated, 0 forwarded
        0 no route, 0 discarded
        Frags: 0 reassemble (0 reassembled, 0 couldn't reassemble)
        0 fragment (0 fragmented, 0 couldn't fragment)
        0 fragment created
 Mcast:        0 received in 0 byte
        0 sent in 0 byte
 Bcast:        0 received, 0 sent
```

6.3 show running-config

A ‘running-config’ consists of a list of commands that, taken together, result in the currently running system configuration.

This list of commands is usually not 100% identical to the list of commands a user has input to configure the device. That is because ‘running-config’ is a textual representation of the system configuration which is stored in binary form in the RAM memory of the device.

Since the effective device configuration is huge, ‘running-config’ in the majority of cases only lists the delta between default settings and current settings. This significantly reduces the amount of output and greatly improves readability of the configuration, but it does require the reader to know what the default settings are.

It is possible, however, to also include values that are at default if the keyword ‘all-defaults’ is appended to the ‘show running-config’ command.

6.3.1 Example: Default vs. Non-default vs. All Defaults

In this example if the speed and duplex settings of an Ethernet interface are at default values (auto-negotiation) then nothing is output. If you change the speed to be fixed at 1Gbps then that value is now non-default and will be output. Duplex is also output, since it is forced to ‘full’ when the speed is fixed at 1Gbps.

```
! Display current configuration for an interface. All settings are at default:
my-device# show running-config interface GigabitEthernet 1/4
Building configuration...
interface GigabitEthernet 1/4
!
end

! Now set the speed to 1Gbps and display the configuration again:
my-device# configure terminal
my-device(config)# interface GigabitEthernet 1/4
my-device(config-if)# speed 1000
my-device(config-if)# end

my-device# show running-config interface GigabitEthernet 1/4
Building configuration...
interface GigabitEthernet 1/4
 speed 1000
 duplex full
!
end

! Include all default settings for that interface:
my-device# show running-config interface GigabitEthernet 1/4 all-defaults
Building configuration...
interface GigabitEthernet 1/4
 switchport voice vlan mode disable
 no switchport voice vlan security
 switchport voice vlan discovery-protocol oui
 loop-protect
 no loop-protect action
 loop-protect tx-mode
 switchport access vlan 1
 switchport trunk native vlan 1
 switchport hybrid native vlan 1
```

```
! ... much output omitted for brevity ...
```

Note how the output of ‘show running-config’ can be restricted to a specific interface. There are several other such filters, described below.

6.3.2 show running-config [all-defaults]

This displays the entire currently running system configuration.

6.3.3 show running-config feature *feature_name* [all-defaults]

Only output the commands relevant to a particular feature. The feature list depends on system configuration and software version. For example:

```
my-device# show running-config feature ?
    <cword>    Valid words are 'GVRP' 'access' 'access-list' 'aggregation'
               'arp-inspection' 'auth' 'clock' 'ddmi' 'dhcp' 'dhcp-snooping'
               'dhcp6_client_interface' 'dhcp_server' 'dns' 'dot1x' 'eps'
               'erps' 'ethersat' 'evc' 'green-ethernet' 'http' 'icli'
               'ip-igmp-snooping' 'ip-igmp-snooping-port'
               'ip-igmp-snooping-vlan' 'ipmc-profile' 'ipmc-profile-range'
               'ipv4' 'ipv6' 'ipv6-mld-snooping' 'ipv6-mld-snooping-port'
               'ipv6-mld-snooping-vlan' 'lacp' 'link-oam' 'lldp' 'logging'
               'loop-protect' 'mac' 'mep' 'mstp' 'mvr' 'mvr-port' 'ntp'
               'perf-mon' 'phy' 'port' 'port-security' 'ptp' 'pvlan' 'qos'
               'rmon' 'snmp' 'source-guard' 'ssh' 'udld' 'user' 'vlan'
               'vtss-rmirror' 'web-privilege-group-level'
my-device# show running-config feature dns
Building configuration...
!
vlan 1
!
!
!
ip dns proxy
!
interface GigabitEthernet 1/1
...
```

The structure of running-config is maintained in the output (i.e., sub-modes such as VLANs and Ethernet interfaces are listed but may be empty if the requested feature is irrelevant for the particular sub-mode).

6.3.4 show running-config interface *list* [all-defaults]

Show running-config for the specific list of Ethernet interfaces. This may contain wildcards, for example:

```
my-device# show running-config interface 10GigabitEthernet *
Building configuration...
interface 10GigabitEthernet 1/1
 speed 1000
 duplex full
!
interface 10GigabitEthernet 1/2
!
end
```

6.3.5 show running-config vlan *list* [all-defaults]

Show running-config for the specific list of VLANs, for example:

```
my-device# show running-config vlan 1-10
Building configuration...
vlan 1
 name default
!
end
```

In this example there is only one VLAN on the system.

6.3.6 show running-config interface vlan *list* [all-defaults]

Show running-config for the specific list of VLAN interfaces, for example:

```
my-device# show running-config interface vlan 1-10
Building configuration...
interface vlan 1
 ip address dhcp fallback 172.16.1.2 255.255.0.0
!
end
```

In this example there is only one VLAN interface on the system.

6.3.7 show running-config line { console | vty } *list* [all-defaults]

Show running-config for the console or list of virtual terminal devices (vty). On current designs there is a single console device, 0. For example:

```
my-device# show running-config line console 0
Building configuration...
line console 0
 exec-timeout 0 0
!
end
```

7 Working with Configuration Files

There are four kinds of configuration files:

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

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

```
copy source destination
```

Copies the source to the destination, where the source and destination can be:

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

```
dir
```

List the contents of the flash: file system

```
more flash: filename
```

Output the contents of the file to the terminal.

```
delete flash: filename
```

Delete the specific file.

7.1 Example: Working With Configuration Files

The following example assumes a file system which contains an additional file called ‘ip’.

```
! List files in flash:
my-device# dir
Directory of flash:
r- 1970-01-01 00:00:00 648 default-config
rw 1970-01-06 03:57:33 1313 startup-config
rw 1970-01-01 19:54:01 1237 ip
3 files, 3198 bytes total.

! Display the contents of the file ‘ip’ (output is abbreviated):
my-device# more flash:ip
hostname my-device
...
end

! Use file ‘ip’ for the next boot by overwriting startup-config:
my-device# copy flash:ip startup-config
% Saving 1237 bytes to flash:startup-config

! Verify that the sizes are identical:
my-device# dir
Directory of flash:
r- 1970-01-01 00:00:00 648 default-config
rw 1970-01-06 05:30:41 1237 startup-config
rw 1970-01-01 19:54:01 1237 ip
3 files, 3122 bytes total.

! Regret and delete startup-config. Note how ‘flash:’ is required:
my-device# delete flash:startup-config
my-device# dir
Directory of flash:
r- 1970-01-01 00:00:00 648 default-config
rw 1970-01-01 19:54:01 1237 ip
2 files, 1885 bytes total.

! Use the currently running config for next boot:
my-device# copy running-config startup-config
Building configuration...
% Saving 1271 bytes to flash:startup-config
```

8 Working with Software Images

The system can store up to two software images that are stored in FLASH. The image selected for bootup is called the *Active* image, while the other is called the *Alternate* image.

It is possible to *swap* the Active and Alternative image, and it is possible to *upgrade* to a new Active image.

A firmware *swap* simply switches the Active/Alternate designation on each image and reboots the system.

A firmware *upgrade* performs these steps:

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

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

The relevant commands are:

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

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

9 CLI Command Groups

The commands are divided into command groups as shown below. Help texts are available in groups and specific commands.

The CLI commands are divided into command groups shown below. Help texts are available on groups and on specific commands

show commands (page 50)

config commands (page 51)

copy commands (page 52)

clear commands (page 52)

Other EXEC commands (page 53)

These command groups are discribed in the following sections.

show commands

The show commands display switch configuration, statistics, and other information.

```
# show ?
    aaa               Authentication, Authorization and Accounting methods
    access            Access management
    access-list       Access list
    aggregation       Aggregation port configuration
    clock             Configure time-of-day clock
    ddmi              DDMI configuration
    dot1x             IEEE Standard for port-based Network Access Control
    eps               Ethernet Protection Switching
    erps              Ethernet Ring Protection Switching
    ethersat          ethersat (Service Activation Test)
    evc               Ethernet Virtual Connections
    green-ethernet    Green ethernet (Power reduction)
    history           Display the session command history
    interface         Interface status and configuration
    ip                Internet Protocol
    ipmc              IPv4/IPv6 multicast configuration
    ipv6              IPv6 configuration commands
    lacp              LACP configuration/status
    line              TTY line information
    link-oam          Link OAM configuration
    lldp              Display LLDP neighbors information.
    logging           System logging message
    loop-protect      Loop protection configuration
    mac               Mac Address Table information
    mep               Maintenance Entity Point
    monitor           Monitoring different system events
    mvr               Multicast VLAN Registration configuration
    network-clock     Show selector state.
    ntp               Configure NTP
    platform          Platform configuration
    port-security     Port Security status - Port Security is a module with no
                      direct configuration.
    privilege         Display command privilege
    process           process
    ptp               Precision time Protocol (1588)
    pvlan             PVLAN configuration
    qos               Quality of Service
    radius-server     RADIUS configuration
    rmon              RMON statistics
    running-config    Show running system information
    snmp              Display SNMP configurations
    spanning-tree     STP Bridge
    switchport        Display switching mode characteristics
    system            system
    tacacs-server     TACACS+ configuration
    terminal          Display terminal configuration parameters
    udld              Uni Directional Link Detection(UDLD) configurations,
                      statistics and status
```

```
    user-privilege    Users privilege configuration
    users             Display information about terminal lines
    version           System hardware and software status
    vlan              VLAN status
    web               Web
# show
```

config commands

Configuration commands allow configuring S4224 features and available options.

```
(config)# ?
    aaa               Authentication, Authorization and Accounting
    access            Access management
    access-list       Access list
    aggregation       Aggregation mode
    banner            Define a login banner
    clock             Configure time-of-day clock
    ddmi              DDMI Information
    default           Set a command to its defaults
    do                To run exec commands in config mode
    dot1x             IEEE Standard for port-based Network Access Control
    enable            Modify enable password parameters
    end               Go back to EXEC mode
    eps               Ethernet Protection Switching.
    erps              Ethernet Ring Protection Switching
    ethersat          ethersat (Service Activation Test)
    evc               Ethernet Virtual Connections
    exit              Exit from current mode
    gvrp              Enable GVRP feature
    help              Description of the interactive help system
    hostname          Set system's network name
    interface         Select an interface to configure
    ip                Internet Protocol
    ipmc              IPv4/IPv6 multicast configuration
    ipv6              IPv6 configuration commands
    lacp              LACP settings
    line              Configure a terminal line
    lldp              LLDP configurations.
    logging           System logging message
    loop-protect      Loop protection configuration
    mac               MAC table entries/configuration
    mep               Maintenance Entity Point
    monitor           Monitoring different system events
    mvr               Multicast VLAN Registration configuration
    network-clock     network-clock
    no                Negate a command or set its defaults
    ntp               Configure NTP
    port-security     Enable/disable port security globally.
    privilege         Command privilege parameters
    ptp               Precision time Protocol (1588)
    qos               Quality of Service
    radius-server     Configure RADIUS
```

```
    rmon             Remote Monitoring
    sharedport       Shared Port status: Internal or External
    snmp-server      Set SNMP server's configurations
    spanning-tree    Spanning Tree protocol
    switchport       Set switching mode characteristics
    tacacs-server    Configure TACACS+
    udld             Enable UDLD in the aggressive or normal mode and to set
                     the configurable message timer on all fiber-optic ports.
    username         Establish User Name Authentication
    vlan             VLAN commands
    web              Web
(config)#
```

copy commands

Copy commands allow transferring or saving configuration files to and from the switch.

```
# copy ?
flash                Copy the File in FLASH or on TFTP server
                     (flash:filename | tftp://server/path-and-filename)
running-config       Copy the currently running configuration
startup-config       Copy the Startup configuration
```

clear commands

Clear commands clear the settings to factory defaults.

```
# clear ?
    access           Access management
    access-list      Access list
    dot1x            IEEE Standard for port-based Network Access Control
    eps              Ethernet Protection Switching.
    erps             Ethernet Ring Protection Switching
    evc              Ethernet Virtual Connections
    ip               Interface Internet Protocol config commands
    ipv6             IPv6 configuration commands
    lacp             Clear LACP statistics
    link-oam         Clear Link OAM statistics
    lldp             Clears LLDP statistics.
    logging          System logging message
    mac              MAC Address Table
    mep              Maintenance Entity Point
    mvr              Multicast VLAN Registration configuration
    network-clock    Clear active WTR timer.
    spanning-tree    STP Bridge
    statistics       Clear statistics for one or more given interfaces
# clear
```

Other EXEC commands

The other EXEC commands include the following.

```
# ?
    clear        Reset functions
    configure    Enter configuration mode
    copy         Copy from source to destination
    delete       Delete one file in flash: file system
    dir          Directory of all files in flash: file system
    disable      Turn off privileged commands
    do           To run exec commands in config mode
    dot1x        IEEE Standard for port-based Network Access Control
    enable       Turn on privileged commands
    exit         Exit from EXEC mode
    firmware     Firmware upgrade/swap
    help         Description of the interactive help system
    ip           IPv4 commands
    ipv6         IPv6 configuration commands
    link-oam     Link OAM configuration
    logout       Exit from EXEC mode
    more         Display file
    no           Negate a command or set its defaults
    ping         Send ICMP echo messages
    ptp          Misc non persistent 1588 settings
    reload       Reload system.
    send         Send a message to other tty lines
    show         Show running system information
    terminal     Set terminal line parameters
    veriphy      Veriphy keyword
#
```

CLI Features and Modes

The software provides an industry-standard CLI with features such as the following (also implemented on the other industry popular Switches/Routers):

- Command history - use of the Up arrow presents the history of commands
- Command-line editing
- Shortcut key options
- Context-sensitive help: gives you the option to press the '**?**' key for a list of valid possible parameters, with descriptions.
- Auto-completion: partially type the keyword and then press the <tab> key; the rest of the keyword is entered automatically.
- Modes - each command can belong to one or more modes. The commands in a particular made can be made invisible in any other mode.

Command modes can include Global Configuration Mode, VLAN Configuration Mode, and Interface Configuration Mode. Examples are provided below.

Global Configuration Mode List

```
1.      aaa              Authentication, Authorization and Accounting
2.      access           Access management
3.      access-list      Access list
4.      aggregation      Aggregation mode
5.      banner           Define a login banner
6.      clock            Configure time-of-day clock
7.      ddmi             DDMI Information
8.      default          Set a command to its defaults
9.      do               To run exec commands in config mode
10.     dot1x            IEEE Standard for port-based Network Access Control
11.     enable           Modify enable password parameters
12.     end              Go back to EXEC mode
13.     eps              Ethernet Protection Switching.
14.     erps             Ethernet Ring Protection Switching
15.     ethersat         ethersat (Service Activation Test)
16.     evc              Ethernet Virtual Connections
17.     exit             Exit from current mode
18.     gvrp             Enable GVRP feature
19.     help             Description of the interactive help system
20.     hostname         Set system's network name
21.     interface        Select an interface to configure
22.     ip               Internet Protocol
23.     ipmc             IPv4/IPv6 multicast configuration
24.     ipv6             IPv6 configuration commands
25.     lacp             LACP settings
26.     line             Configure a terminal line
27.     lldp             LLDP configurations.
28.     logging          System logging message
29.     loop-protect     Loop protection configuration
30.     mac              MAC table entries/configuration
31.     mep              Maintenance Entity Point
32.     monitor          Monitoring different system events
33.     mvr              Multicast VLAN Registration configuration
34.     network-clock    network-clock
35.     no               Negate a command or set its defaults
36.     ntp              Configure NTP
37.     port-security    Enable/disable port security globally.
38.     privilege        Command privilege parameters
39.     ptp              Precision time Protocol (1588)
40.     qos              Quality of Service
41.     radius-server    Configure RADIUS
42.     rmon             Remote Monitoring
43.     sharedport       Shared Port status: Internal or External
44.     snmp-server      Set SNMP server's configurations
45.     spanning-tree    Spanning Tree protocol
46.     switchport       Set switching mode characteristics
47.     tacacs-server    Configure TACACS+
48.     udld             Enable UDLD in the aggressive or normal mode and to set
49.                      the configurable message timer on all fiber-optic ports.
50.     username         Establish User Name Authentication
51.     vlan             VLAN commands
```

```
52.     web             Web
```

VLAN Configuration Mode Example

```
(config)# vlan 100
(config-vlan)# ?
do      To run exec commands in config mode
end     Go back to EXEC mode
exit    Exit from current mode
help    Description of the interactive help system
name    ASCII name of the VLAN
no
```

Interface Configuration Mode Example

```
1.    access-list           Access list
2.    aggregation           Create an aggregation
3.    ddmi
4.    description
5.    do                    To run exec commands in config mode
6.    dot1x                 IEEE Standard for port-based Network Access Control
7.    duplex                Interface duplex
8.    end                   Go back to EXEC mode
9.    evc                   Ethernet Virtual Connections
10.   excessive-restart     Restart backoff algorithm after 16 collisions (No
11.                             excessive-restart means discard frame after 16
12.                             collisions)
13.   exit                  Exit from current mode
14.   flowcontrol           Traffic flow control.
15.   green-ethernet        Green ethernet (Power reduction)
16.   gvrp                  Enable GVRP on port(s)
17.   help                  Description of the interactive help system
18.   ip                    Internet Protocol
19.   ipv6                  IPv6 configuration commands
20.   lacp                  Enable LACP on this interface
21.   link-oam              Enable or Disable(when the no keyword is entered)
                             Link OAM on the interface
22.   lldp                  LLDP configurations.
23.   loop-protect          Loop protection configuration on port
24.   mac                   MAC keyword
25.   media-type            Media type.
26.   mtu                   Maximum transmission unit
27.   mvr                   Multicast VLAN Registration configuration
28.   network-clock         network-clock
29.   no                    Negate a command or set its defaults
30.   platform
31.   port-security         Enable/disable port security per interface.
32.   ptp                   Precision time Protocol (1588)
33.   pvlan                 Private VLAN
34.   qos                   Quality of Service
35.   rmon                  Configure Remote Monitoring on an interface
```

```
36.   shutdown              Shutdown of the interface.
37.   snmp-server           Set SNMP server's configurations
38.   spanning-tree         Spanning Tree protocol
39.   speed                 Configures interface speed. If you use 10, 100, or
                            1000 keywords with the auto keyword the port will
                             only advertise the specified speeds.
40.   switchport            Switching mode characteristics
41.   udld                  UDLD configurations.
```

Privilege Levels

A set of privilege attributes may be assigned to each command based on the level configured.
A command cannot be accessed or executed if the logged in user does not have a sufficient privilege assigned.

User EXEC Mode (> Prompt)

The User EXEC mode is the initial mode available for the users for the insufficient privileges. The User EXEC mode contains a limited set of commands. The command prompt shown at this level is:

```
>
```

Privileged EXEC Mode (# Prompt)

The administrator/user must enter the Privileged EXEC mode in order to have access to the full suite of commands. The Privileged EXEC mode requires password authentication using an ‘enable’ command if set. The command prompt shown at this level is:

```
#
```

Keyword Abbreviations

Any keyword can be accepted just by typing an unambiguous prefix (e.g., by typing "sh" for "show" in the example below):

```
# sh ip route
0.0.0.0/0 via VLAN1:10.9.61.1 <UP GATEWAY HW_RT>
10.9.61.0/24 via VLAN1 <UP HW_RT>
127.0.0.1/32 via OS:lo:127.0.0.1 <UP HOST>
224.0.0.0/4 via OS:lo:127.0.0.1 <UP>
```

Error Checking

Before executing a command, the CLI checks that the current mode is still valid, the user has sufficient privilege, and all parameters entered are within the valid range among others. You are alerted to the error by a caret displayed under the offending word along with an error message.

```
(config)# clock summer-1 time PDT date 14
                                        ^
% Invalid word detected at '^' marker.
```

The “no” Form of Commands

Every configuration command has a “no” form to negate or set its default.In general, the no form is used to reverse the action of a command or reset a value back to the default. For example, the ‘no ip routing’ configuration command reverses the ‘ip routing’ of an interface.

Industry-standard Configuration Support

The software supports an industry-standard configuration where the commands are stored in a text format.The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the S4224.

There are three system files:

running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.

startup-config: The startup configuration for the switch, read at boot time.

default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings. This is a per-build customizable file that does not require C source code changes.

It is also possible to store up to four other files and apply them to the running-config, thereby switching configuration. The maximum number of files in the configuration file is limited to a compressed size which does not exceed approximately 1MB.

The configuration made can be dynamically viewed by entering the `show running-config` command. This current running configuration may be copied to the startup configuration using the `copy` command.

This industry-standard file may be edited and can be populated on multiple other switches using any standard text editor offline.

Sample running-config File

```
# show running-config
Building configuration...
username admin privilege 15 password none
!
vlan 1
 name default
!
vlan 201
!
ip route 0.0.0.0 0.0.0.0 10.9.61.1
ip name-server 10.9.60.92
ip dns proxy
ntp enable
ntp server 1 ip-address time.nist.gov
clock summer-time PDT recurring 2 7 3 02:00 1 7 11 02:00 60
clock timezone PDT -8
spanning-tree mst name 00-01-c1-00-b5-60 revision 0
green-ethernet led on-event link-change 2
green-ethernet led on-event error
green-ethernet led interval 17-8 intensity 10
no lldp tlv-select system-capabilities
snmp-server contact billyjoe
snmp-server location Level4_T3
voice vlan oui 00-01-E3 description Siemens AG phones
voice vlan oui 00-03-6B description Cisco phones
voice vlan oui 00-0F-E2 description H3C phones
voice vlan oui 00-60-B9 description Philips and NEC AG phones
voice vlan oui 00-D0-1E description Pingtel phones
voice vlan oui 00-E0-75 description Polycom phones
voice vlan oui 00-E0-BB description 3Com phones
network-clock wait-to-restore 5
ptp 0 mode boundary twostep ethernet twoway id
00:01:c1:ff:fe:00:b5:60 vid 1 0
ptp 0 ho filter 60 adj-threshold 60
!
interface GigabitEthernet 1/1
 switchport hybrid allowed vlan 1
 switchport hybrid port-type c-port
 switchport mode hybrid
 lldp transmit
!
interface GigabitEthernet 1 1/2
 switchport hybrid allowed vlan 201-264
 switchport hybrid port-type c-port
 switchport mode hybrid
 green-ethernet eee
 green-ethernet eee urgent-queue 3,6
 no spanning-tree
!
interface GigabitEthernet 1/3
 switchport hybrid allowed vlan 201-264
```

```
 switchport hybrid port-type c-port
 switchport mode hybrid
 no lldp receive
 no lldp transmit
 green-ethernet eee urgent-queue 4
 green-ethernet short-reach
!
interface GigabitEthernet 1/4
 switchport hybrid allowed vlan 201-264
 switchport hybrid port-type c-port
 switchport mode hybrid
 no lldp receive
 no lldp transmit
 no spanning-tree
!
interface GigabitEthernet 1/5
 switchport hybrid allowed vlan none
 switchport hybrid port-type c-port
 switchport mode hybrid
 lldp receive
 thermal-protect port-prio 2
 no spanning-tree
!
interface GigabitEthernet 1/6
 switchport hybrid allowed vlan none
 switchport hybrid port-type c-port
 switchport mode hybrid
 no lldp receive
  no lldp transmit
!
interface GigabitEthernet 1/7
 switchport hybrid allowed vlan none
 switchport hybrid port-type c-port
 switchport mode hybrid
 no lldp receive
 no lldp transmit
 no spanning-tree
!
interface GigabitEthernet 1/8
 no loop-protect tx-mode
 switchport hybrid allowed vlan none
 switchport hybrid port-type c-port
 switchport mode hybrid
 no lldp receive
 no lldp transmit
 no spanning-tree
 spanning-tree edge
!
interface GigabitEthernet 1/9
 switchport hybrid allowed vlan none
 switchport hybrid port-type c-port
 switchport mode hybrid
 no lldp receive
```

```
 no lldp transmit
 no spanning-tree
!
interface 10GigabitEthernet 1/1
 loop-protect action shutdown log
 switchport hybrid allowed vlan none
 switchport hybrid port-type c-port
 switchport mode hybrid
 no spanning-tree
spanning-tree edge
!
interface vlan 1
 ip address 10.9.61.132 255.255.255.0
!
mep 1 down domain port flow 3 level 1 interface GigabitEthernet 1/3
mep 1 vid 111
mep 1 peer-mep-id 2 mac 00-01-C1-00-B1-D4
mep 1 cc 0
mep 1 aps 0 raps
mep 2 down domain port flow 4 level 1 interface GigabitEthernet 1/4
mep 2 mep-id 2
mep 2 vid 111
mep 2 peer-mep-id 1 mac 00-01-C1-00-B5-73
mep 2 cc 0
mep 2 aps 0 raps
erps 1 major port0 interface Gi 1/3 port1 interface Gi 1/4
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
erps                          1                                    vlan
201,202,203,204,205,206,207,208,209,210,211,212,213,214,215,216
,217,218,219,220,221,222,223,224,225,226,227,228,229,230,231,23
2,233,234,235,236,237,238,239,240,241,242,243,244,245,246,247,2
48,249,250,251,252,253,254,255,256,257,258,259,260,261,262,263
!
!
28 line console 0
 exec-timeout 0 0
 length 0
 width 0
!
line vty 0
```

```
# show running-config
Building configuration...
username admin privilege 15 password none
!
vlan 1
!
!
!
spanning-tree mst name 00-c0-f2-00-00-01 revision 0
!
interface GigabitEthernet 1/1
!
```

```
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
!
interface GigabitEthernet 1/4
!
interface 10GigabitEthernet 1/1
!
interface 10GigabitEthernet 1/2
!
interface vlan 1
 ip address 192.168.0.1 255.255.255.0
!
!
spanning-tree aggregation
 spanning-tree link-type point-to-point
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
end
#
```

10 CLI Command Descriptions

CLI Command Groups

The TN device firmware lets a network admininstrator perform a comprehensive set of management functions via the web GUI, CLI (command line interface) or SNMP.

The TN device supports an industry-standard configuration command structure letting you configure and view device configurations via serial console, Telnet, or SSH access.

The TN CLI commands are documented in the separate groups as shown below. Help text is available for CLI command groups and for individual CLI commands.

?	Help list of commands (page 64)
clear	Reset functions (page 69)
configure	Enter configuration mode (page 71)
copy	Copy from source to destination (page 297)
delete	Delete one file in flash: file system (page 298)
dir	Directory of all files in flash: file system (page 298)
disable	Turn off privileged commands (page 299)
do	To run exec commands in config mode (page 300)
dot1x	IEEE Standard for port-based Network Access Control (page 301)
enable	Turn on privileged commands mode (page 301)
exit	Exit from EXEC mode (page 304)
firmware	Firmware upgrade/swap (page 305)
help	Description of the interactive help system (page 307)
ip	IPv4 commands (page 308)
ipv6	IPv6 configuration commands (page 308)
link-oam	Link OAM configuration (page 310)
logout	Exit from EXEC mode (page 311)
more	Display file (page 311)
no	Negate a command or set its defaults (page 312)
ping	Send ICMP echo messages (page 313)
ptp	Misc non persistent 1588 settings (page 232)
reload	Reload system (page 317)
send	Send a message to other tty lines (page 318)
show	Show running system information (page 350)
terminal	Set terminal line parameters (page 351)
veriphy	Veriphy keyword (page 472)

Note that not all CLI commands are available or supported on all TN device models.

CLI Commands

The individual commands in each group are described in the following sections.

? Help List of Commands

Command: ?

Mode: Any (Exec, Privileged Exec and Config)

Syntax: **?**

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

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

Example:

```
# ?
  clear       Reset functions
  configure   Enter configuration mode
  copy        Copy from source to destination
  delete      Delete one file in flash: file system
  dir         Directory of all files in flash: file system
  disable     Turn off privileged commands
  do          To run exec commands in config mode
  dot1x       IEEE Standard for port-based Network Access Control
  enable      Turn on privileged commands
  exit        Exit from EXEC mode
  firmware    Firmware upgrade/swap
  help        Description of the interactive help system
  ip          IPv4 commands
  ipv6        IPv6 configuration commands
  link-oam    Link OAM configuration
  logout      Exit from EXEC mode
  more        Display file
  no          Negate a command or set its defaults
  ping        Send ICMP echo messages
  ptp         Misc non persistent 1588 settings
  reload      Reload system.
  send        Send a message to other tty lines
  show        Show running system information
  terminal    Set terminal line parameters
  veriphy     Veriphy keyword
# ??
# ?
1.    clear access management statistics
2.    clear access-list ace statistics
3.    clear dot1x statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]
4.    clear eps <inst> wtr
5.    clear erps [ <groups> ] statistics
6.    clear evc statistics { [ <evc_id> | all ] } [ ece [ <ece_id> ] ] [ interface ( <port_type> [ <port_list> ] ) ] [ pw <pw_num_list> ]
7.    clear ip arp
8.    clear ip dhcp detailed statistics { server | client | snooping | relay | helper | all } [ interface ( <port_type> [ <in_port_list> ] ) ]
9.    clear ip dhcp relay statistics
10.   clear ip dhcp server binding <ip>
11.   clear ip dhcp server binding { automatic | manual | expired }
12.   clear ip dhcp server statistics
13.   clear ip dhcp snooping statistics [ interface ( <port_type> [ <in_port_list> ] ) ]
14.   clear ip igmp snooping [ vlan <v_vlan_list> ] statistics
15.   clear ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]
```

16. clear ipv6 mld snooping [vlan <v_vlan_list>] statistics
17. clear ipv6 neighbors
18. clear ipv6 statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]
19. clear lacp statistics
20. clear link-oam statistics [interface (<port_type> [<plist>])]
21. clear lldp statistics { [interface (<port_type> [<plist>])] | global }
22. clear logging [informational] [notice] [warning] [error] [switch <switch_list>]
23. clear mac address-table
24. clear mep <inst> { lm | dm | tst | bfd }
25. clear mvr [vlan <v_vlan_list> | name <mvr_name>] statistics
26. clear network-clock clk-source <clk_list>
27. clear spanning-tree { { statistics [interface (<port_type> [<v_port_type_list>])] } | { detected-protocols [interface (<port_type> [<v_port_type_list_1>])] } }
28. clear statistics [interface] (<port_type> [<v_port_type_list>])
29. configure terminal
30. copy { startup-config | running-config | <source_path> } { startup-config | running-config | <destination_path> } [syntax-check]
31. delete <path>
32. dir
33. disable [<new_priv>]
34. do <command>
35. dot1x initialize [interface (<port_type> [<plist>])]
36. enable [<new_priv>]
37. exit
38. firmware swap
39. firmware upgrade <tftpserver_path_file> [activate { now | defer }]
40. help
41. ip dhcp retry interface vlan <vlan_id>
42. ipv6 dhcp-client restart [interface vlan <v_vlan_list>]
43. link-oam remote-loopback { start | stop } interface (<port_type> [<v_port_type_list>])
44. logout
45. more <path>
46. no debug interrupt-monitor source <source>
47. no debug ipv6 nd
48. no debug trace hunt
49. no port-security shutdown [interface (<port_type> [<v_port_type_list>])]
50. no ptp <clockinst> wireless mode interface (<port_type> [<v_port_type_list>])
51. no terminal editing
52. no terminal exec-timeout
53. no terminal history size
54. no terminal length
55. no terminal width
56. ping ip { <v_ip_addr> | <v_ip_name> } [repeat <count>] [size <size>] [interval <seconds>]
57. ping ipv6 { <v_ipv6_addr> | <v_ipv6_name> } [repeat <count>] [size <size>] [interval <seconds>] [interface vlan <v_vlan_id>]
58. ptp <clockinst> local-clock { update | ratio <ratio> }
59. ptp <clockinst> wireless delay <base_delay> [<incr_delay>] interface (<port_type> [<v_port_type_list>])
60. ptp <clockinst> wireless mode interface (<port_type> [<v_port_type_list>])
61. ptp <clockinst> wireless pre-notification interface (<port_type> [<v_port_type_list>])
62. reload { { { cold | warm } [sid <usid>] } | { defaults [keep-ip] } }
63. send { * | <session_list> | console 0 | vty <vty_list> } <message>
64. show aaa
65. show access management [statistics | <access_id_list>]
66. show access-list [interface [(<port_type> [<v_port_type_list>])]] [rate-limiter [<rate_limiter_list>]] [ace statistics [<ace_list>]]
67. show access-list ace-status [static] [link-oam] [loop-protect] [dhcp] [ptp] [upnp] [arp-inspection] [evc] [mep] [ipmc] [ip-source-guard] [ip-mgmt] [conflicts] [switch <switch_list>]
68. show aggregation [mode]
69. show clock
70. show clock detail
71. show ddmi
72. show dot1x statistics { eapol | radius | all } [interface (<port_type> [<v_port_type_list>])]
73. show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief]
74. show eps [<inst>] [detail]
75. show erps { [<groups>] } [detail | statistics]

76. show ethersat config
77. show ethersat loopback { config | state | testsideport | smac | vid | timeout }
78. show ethersat loopback { status }
79. show ethersat profile <pid> config
80. show ethersat profile <pid> frameformat
81. show evc statistics { [<evc_id> | all] } [ece [<ece_id>]] [interface (<port_type> [<port_list>])] [pw <pw_num_list>] [cos <cos>] [green | yellow | red | discard] [frames | bytes]
82. show evc { [<evc_id> | all] } [ece [<ece_id>]]
83. show green-ethernet [interface (<port_type> [<port_list>])]
84. show green-ethernet energy-detect [interface (<port_type> [<port_list>])]
85. show green-ethernet short-reach [interface (<port_type> [<port_list>])]
86. show history
87. show interface (<port_type> [<in_port_list>]) switchport [access | trunk | hybrid]
88. show interface (<port_type> [<plist>]) transceiver
89. show interface (<port_type> [<v_port_type_list>]) capabilities
90. show interface (<port_type> [<v_port_type_list>]) statistics [{ packets | bytes | errors | discards | filtered | { priority [<priority_v_0_to_7>] } }] [{ up | down }]
91. show interface (<port_type> [<v_port_type_list>]) status
92. show interface (<port_type> [<v_port_type_list>]) veriphy
93. show interface vlan [<vlist>]
94. show ip arp
95. show ip arp inspection [interface (<port_type> [<in_port_type_list>]) | vlan <in_vlan_list>]
96. show ip arp inspection entry [dhcp-snooping | static] [interface (<port_type> [<in_port_type_list>])]
97. show ip dhcp detailed statistics { server | client | snooping | relay | normal-forward | combined } [interface (<port_type> [<in_port_list>])]
98. show ip dhcp excluded-address
99. show ip dhcp pool [<pool_name>]
100. show ip dhcp relay [statistics]
101. show ip dhcp server
102. show ip dhcp server binding <ip>
103. show ip dhcp server binding [state { allocated | committed | expired }] [type { automatic | manual | expired }]
104. show ip dhcp server declined-ip
105. show ip dhcp server declined-ip <declined_ip>
106. show ip dhcp server statistics
107. show ip dhcp snooping [interface (<port_type> [<in_port_list>])]
108. show ip dhcp snooping table
109. show ip domain
110. show ip http server secure status
111. show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
112. show ip igmp snooping mrouter [detail]
113. show ip interface brief
114. show ip name-server
115. show ip route
116. show ip source binding [dhcp-snooping | static] [interface (<port_type> [<in_port_type_list>])]
117. show ip ssh
118. show ip statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]
119. show ip verify source [interface (<port_type> [<in_port_type_list>])]
120. show ipmc profile [<profile_name>] [detail]
121. show ipmc range [<entry_name>]
122. show ipv6 dhcp-client [interface vlan <v_vlan_list>]
123. show ipv6 interface [vlan <v_vlan_list> { brief | statistics }]
124. show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
125. show ipv6 mld snooping mrouter [detail]
126. show ipv6 neighbor [interface vlan <v_vlan_list>]
127. show ipv6 route [interface vlan <v_vlan_list>]
128. show ipv6 statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]
129. show lacp { internal | statistics | system-id | neighbor }
130. show line [alive]
131. show link-oam { [status] [link-monitor] [statistics] } [interface (<port_type> [<plist>])]
132. show lldp med media-vlan-policy [<v_0_to_31>]
133. show lldp med remote-device [interface (<port_type> [<port_list>])]
134. show lldp neighbors [interface (<port_type> [<v_port_type_list>])]
135. show lldp statistics [interface (<port_type> [<v_port_type_list>])]

136. show logging <log_id> [switch <switch_list>]
137. show logging [informational] [notice] [warning] [error] [switch <switch_list>]
138. show loop-protect [interface (<port_type> [<plist>])]
139. show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>]) | vlan <v_vlan_id_2>] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]
140. show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck | pm | syslog | tlv | bfd | rt | lst] [detail]
141. show monitor [session { <session_number> | all | remote }]
142. show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
143. show network-clock
144. show network-clock clock-selection-config
145. show network-clock source-nomination-config
146. show network-clock station-clock-config
147. show network-clock synchronization
148. show ntp status
149. show platform phy [interface (<port_type> [<v_port_type_list>])]
150. show platform phy id [interface (<port_type> [<v_port_type_list>])]
151. show platform phy instance
152. show platform phy mode [interface (<port_type> [<v_port_type_list>])]
153. show port-security port [interface (<port_type> [<v_port_type_list>])]
154. show port-security switch [interface (<port_type> [<v_port_type_list>])]
155. show privilege
156. show process list [detail]
157. show process load
158. show ptp <clockinst> local-clock
159. show ptp <clockinst> slave-cfg
160. show ptp <clockinst> slave-table-unicast
161. show ptp <clockinst> { default | current | parent | time-property | filter | servo | clk | ho | uni | master-table-unicast | slave | { { port-state | port-ds | wireless | foreign-master-record } [interface (<port_type> [<v_port_type_list>])] } }
162. show ptp ext-clock
163. show ptp system-time
164. show pvlan [<pvlan_list>]
165. show pvlan isolation [interface (<port_type> [<plist>])]
166. show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]
167. show radius-server [statistics]
168. show rmon alarm [<id_list>]
169. show rmon event [<id_list>]
170. show rmon history [<id_list>]
171. show rmon statistics [<id_list>]
172. show running-config [all-defaults]
173. show running-config feature <feature_name> [all-defaults]
174. show running-config interface (<port_type> [<list>]) [all-defaults]
175. show running-config interface vlan <list> [all-defaults]
176. show running-config line { console | vty } <list> [all-defaults]
177. show running-config vlan <list> [all-defaults]
178. show snmp
179. show snmp access [<group_name> { v1 | v2c | v3 | any } { auth | noauth | priv }]
180. show snmp community v3 [<community>]
181. show snmp host [<conf_name>] [system] [switch] [interface] [aaa]
182. show snmp mib context
183. show snmp mib ifmib ifIndex
184. show snmp security-to-group [{ v1 | v2c | v3 } <security_name>]
185. show snmp user [<username> <engineID>]
186. show snmp view [<view_name> <oid_subtree>]
187. show spanning-tree [summary | active | { interface (<port_type> [<v_port_type_list>]) } | { detailed [interface (<port_type> [<v_port_type_list_1>])] } | { mst [configuration | { <instance> [interface (<port_type> [<v_port_type_list_2>])] }] }]
188. show switchport forbidden [{ vlan <vid> } | { name <name> }]
189. show system cpu status
190. show tacacs-server
191. show terminal
192. show udld [interface (<port_type> [<plist>])]

```
193.  show user-privilege
194.  show users [ myself ]
195.  show version [ brief ]
196.  show vlan [ id <vlan_list> | name <name> | brief ] [ all ]
197.  show vlan ip-subnet [ <ipv4> ]
198.  show vlan mac [ address <mac_addr> ]
199.  show vlan protocol [ eth2 { <etype> | arp | ip | ipx | at } ] [ snap { <oui> | rfc-1042 | snap-8021h } <pid> ] [ llc <dsap> <ssap> ]
200.  show vlan status [ interface ( <port_type> [ <plist> ] ) ] [ admin | all | combined | conflicts | erps | evc | gvrp | mep | mstp | mvr | nas | rmirror | vcl | voice-vlan ]
201.  show web privilege group [ <group_name> ] level
202.  terminal editing
203.  terminal exec-timeout <min> [ <sec> ]
204.  terminal help
205.  terminal history size <history_size>
206.  terminal length <lines>
207.  terminal width <width>
208.  veriphy [ { interface ( <port_type> [ <v_port_type_list> ] ) } ]
209.  #
#
```

Clear (Reset) Commands

Command: Clear

Mode: **#** *(*Privileged Exec)

Syntax: **clear**

Description: Reset a specific function to reset to factory defaults.

Example:

```
# clear ?
    access           Access management
    access-list      Access list
    dot1x            IEEE Standard for port-based Network Access Control
    eps              Ethernet Protection Switching.
    erps             Ethernet Ring Protection Switching
    evc              Ethernet Virtual Connections
    ip               Interface Internet Protocol config commands
    ipv6             IPv6 configuration commands
    lacp             Clear LACP statistics
    link-oam         Clear Link OAM statistics
    lldp             Clears LLDP statistics.
    logging          System logging message
    mac              MAC Address Table
    mep              Maintenance Entity Point
    mvr              Multicast VLAN Registration configuration
    network-clock    Clear active WTR timer.
    spanning-tree    STP Bridge
    statistics       Clear statistics for one or more given interfaces
# clear
```

Parameters:

```
# clear??
clear access management statistics
clear access-list ace statistics
clear dot1x statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]
clear eps <inst> wtr
clear erps [ <groups> ] statistics
clear evc statistics { [ <evc_id> | all ] } [ ece [ <ece_id> ] ] [ interface ( <port_type> [ <port_list> ]
       ) ] [ pw <pw_num_list> ]
clear ip arp
clear ip dhcp detailed statistics { server | client | snooping | relay | helper | all } [ interface (
      <port_type> [ <in_port_list> ] ) ]
clear ip dhcp relay statistics
clear ip dhcp server binding <ip>
clear ip dhcp server binding { automatic | manual | expired }
clear ip dhcp server statistics
clear ip dhcp snooping statistics [ interface ( <port_type> [ <in_port_list> ] ) ]
clear ip igmp snooping [ vlan <v_vlan_list> ] statistics
clear ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]
clear ipv6 mld snooping [ vlan <v_vlan_list> ] statistics
clear ipv6 neighbors
clear ipv6 statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]
clear lacp statistics
clear link-oam statistics [ interface ( <port_type> [ <plist> ] ) ]
```

```
clear lldp statistics { [ interface ( <port_type> [ <plist> ] ) ] | global }
clear logging [ informational ] [ notice ] [ warning ] [ error ] [ switch <switch_list> ]
clear mac address-table
clear mep <inst> { lm | dm | tst | bfd }
clear mvr [ vlan <v_vlan_list> | name <mvr_name> ] statistics
clear network-clock clk-source <clk_list>
clear spanning-tree { { statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ] } | { detected-
      protocols [ interface ( <port_type> [ <v_port_type_list_1> ] ) ] } }
clear statistics [ interface ] ( <port_type> [ <v_port_type_list> ] )
# clear
```

Config Commands

Config commands let you configure the device's available features and options. Use the **config** command to enter configuration mode.

Command: Configure Terminal Mode

Mode: (config)

Syntax: **configure**

Description: Enter configuration mode. The prompt turns from # to (config)#. Use the exit command to return to the previous mode.

Example:

```
# configure terminal
(config)#
```

These **config** commands are available in config mode.

```
# con ter
(config)#<tab>
aaa             access          access-list     aggregation     banner
clock           ddmi            default         do              dot1x
enable          end             eps             erps            ethersat
evc             exit            gvrp            help            hostname
interface       ip              ipmc            ipv6            lacp
line            lldp            logging         loop-protect    mac
mep             monitor         mvr             network-clock   no
ntp             port-security   privilege       ptp             qos
radius-server   rmon            sharedport      snmp-server     spanning-tree
switchport      tacacs-server   udld            username        vlan
web
(config)#
```

The **config** commands are described in the following sections.

Command: Configure AAA

Syntax:
aaa accounting { console | telnet | ssh } tacacs { [commands <priv_lvl>] [exec] }*1
aaa authentication login { console | telnet | ssh | http } { { local | radius |tacacs } [{ local | radius | tacacs } [{ local | radius | tacacs }]] }
aaa authorization { console | telnet | ssh } tacacs commands <priv_lvl> [config-commands]

Description: Configure Accounting, Authentication, and Authorization. The authentication commands allow you to configure how a user is authenticated when s/he logs into the switch via one of the management client interfaces. The authorization commands allow you to limit the CLI commands available to a user. The accounting commands allow you to configure command and exec (login) accounting.

The S4224 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.

Methods that involve remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.

Mode: (config)#

Example 1: Configure Accounting:

```
(config)# aaa accounting??
aaa accounting { console | telnet | ssh } tacacs { [ commands <priv_lvl> ] [ exec ] }*1
(config)# aaa accounting console ?
    tacacs    Use TACACS+ for accounting
(config)# aaa accounting console tacacs ?
    commands    Enable command accounting
    exec        Enable EXEC accounting
(config)# aaa accounting console tacacs commands ?
    <0-15>    Command privilege level. Commands >= this level are accounted
(config)# aaa accounting console tacacs commands 15 ?
    exec    Enable EXEC accounting
    <cr>
(config)# aaa accounting console tacacs commands 15
```

Example 2: Configure Authentication:

```
(config)# aaa authentication ?
    login    Login
(config)# aaa authentication login ?
    console    Configure Console authentication
    http       Configure HTTP authentication
    ssh        Configure SSH authentication
    telnet     Configure Telnet authentication
(config)# aaa authentication login console ?
    local     Use local database for authentication
    radius    Use RADIUS for authentication
    tacacs    Use TACACS+ for authentication
(config)# aaa authentication login http ?
    local     Use local database for authentication
    radius    Use RADIUS for authentication
```

```
    tacacs    Use TACACS+ for authentication
(config)# aaa authentication login ssh ?
    local     Use local database for authentication
    radius    Use RADIUS for authentication
    tacacs    Use TACACS+ for authentication
(config)# aaa authentication login telnet ?
    local     Use local database for authentication
    radius    Use RADIUS for authentication
    tacacs    Use TACACS+ for authentication
(config)# aaa authentication login telnet
```

Example 3: Configure Authorization and show resulting AAA config:

```
(config)# aaa authorization ?
    console    Configure Console command authorization
    ssh        Configure SSH command authorization
    telnet     Configure Telnet command authorization
(config)# aaa authorization console ?
    tacacs    Use TACACS+ for authorization
(config)# aaa authorization ssh ?
    tacacs    Use TACACS+ for authorization
(config)# aaa authorization telnet ?
    tacacs    Use TACACS+ for authorization
(config)# aaa authorization telnet tacacs ?
    commands    Enable command authorization
(config)# aaa authorization telnet tacacs commands ?
    <0-15>    Command privilege level. Commands >= this level are authorized
(config)# aaa authorization telnet tacacs commands 15 ?
    config-commands    Include configuration commands
    <cr>
(config)# aaa authorization console tacacs commands 15 config-commands ?
<cr>
(config)# aaa authorization console tacacs commands 15 config-commands
(config)# end
# show aaa
Authentication :
  console : local
  telnet  : local
  ssh     : local
  http    : local
Authorization :
  console : tacacs, commands 15 enabled, config-commands enabled
  telnet  : no, commands disabled
  ssh     : no, commands disabled
Accounting :
  console : no, commands disabled, exec disabled
  telnet  : no, commands disabled, exec disabled
  ssh     : no, commands disabled, exec disabled
#
```

Problem: With TACACS+ accounting enabled, the command privilege level filtering option does not always work as expected. At the default level of 0, all commands are logged as expected. After setting the level to 1, which should log commands level 1 and above, some level 5 commands are not logged. This includes, but is not limited to, "Show IP", "Show Clock", and "Show System". Other level 5 commands such as "Show SNMP" and "Show Spanning Tree" continue to be logged even after the filter is set above level 5.
Workaround: This problem does not effect the ability to log commands; a work around is to edit/filter the accounting log on the TACACS server.

Message: *Command Authorization Failure*
Problem: TACACS+ Command Authorization does not allow config command execution.
Description: When TACACS+ Command Authorization is turned on, it not possible to execute configuration commands (ex. "config term"). The error message "*Command Authorization Failure*" is displayed on the CLI. This is true even when the "Cfg Cmd" checkbox is unchecked which should inhibit authorization.
Workaround: A fix for this problem is in process.

Command: Configure Access Management

Syntax: **access management** <access_id> <access_vid> <start_addr> [to <end_addr>] { [web] [snmp] [telnet] | all }

Description: Configure Access management.The maximum number of Access Management filter entries allowed is 16. If the application's type matches any one of the access management entries, it will allow access to the S4224. The parameters are:
access_id : The ID of access management entry (1-16).
access_vid : The VLAN ID for the access management entry (1-4095).
start_addr : Start IPv4 address.
to : the address range end address <end_addr> .
web Web service.
snmp SNMP service.
all All services (Web, SNMP and Telnet).

Mode: (config)#

Example: Display the command options and display the current config:

```
(config)# access management ?
    <1-16>    ID of access management entry
    <cr>
(config)# access management 1 ?
    <1-4094>    The VLAN ID for the access management entry
(config)# access management 1 10 ?
    <ipv4_addr>    Start IPv4 address
    <ipv6_addr>    Start IPv6 address
(config)# access management 1 10 192.168.1.110 ?
    all       All services
    snmp      SNMP service
    telnet    TELNET/SSH service
    to        End address of the range
    web       Web service
    <cr>
(config)# access management 1 10 192.168.1.110 all ?
    <cr>
(config)# access management 1 10 192.168.1.110 snmp ?
    all       All services
    telnet    TELNET/SSH service
    web       Web service
    <cr>
(config)# access management 1 10 192.168.1.110 snmp all ?
    <cr>
(config)# access management 1 10 192.168.1.110 snmp telnet ?
    all     All services
    web     Web service
    <cr>
(config)# access management 1 10 192.168.1.110 snmp web ?
    telnet    TELNET/SSH service
    <cr>
(config)# access management 1 10 192.168.1.110 snmp web
#
```

Messages: (config)# **access management 1 1 192.168.1.110**
% At least one service must be selected.

HTTP/HTTPS: Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.
SNMP: Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.
TELNET/SSH: Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

Command: Configure Access List ACE

Syntax: **config access-list ace**

Description: Configure access list ACE parameters. Note that the ACL rate limiter and EVC policer can not both be enabled. The Access Control List consists of a table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL.

The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.The ACE will only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. There can be 16 different ACL rate limiters. A Rate Limiter ID could be assigned to the ACE(s) or ingress port(s). An ACE consists of several parameters, which vary by the frame type selected. The ingress port must be selected for the ACE, and then the frame type.

Different parameter options are displayed based on the frame type selected. Note that:

- additional MAC and EtherType parameters are available for ACE config when the Frame Type chosen is 'EtherType' match.
- additional MAC and ARP parameters are available for ACE config when the Frame Type is chosen as 'ARP' match.
- additional MAC and ARP parameters are available for ACE config when the Frame Type is chosen as 'IP' match.
- additional parameters are available for config when the IP Protocol Filter is selected as ICMP.
- additional parameters are available for config when the IP Protocol Filter is selected as UDP.
- additional parameters are available for config when the IP Protocol Filter is selected as TCP.

Mode: (config)#

Example 1: Display the various config access-list ace functions:

```
(config)# access-list ace ?
    < 1-512>          ACE ID
    update            Update an existing ACE
(config)# access-list ace 1 ?
    action          Access list action
    dmac-type       The type of destination MAC address
    frame-type      Frame type
    ingress         Ingress
    logging         Logging frame information. Note: The logging feature only
                    works when the packet length is less than 1518 (without
                    VLAN tags) and the System Log memory size and logging rate
                    is limited.
    next            insert the current ACE before the next ACE ID
    policy          Policy
    rate-limiter    Rate limiter
    redirect        Redirect frame to specific port
    shutdown        Shutdown incoming port. The shutdown feature only works
                    when the packet length is less than 1518 (without VLAN
                    tags).
    tag-priority    Tag priority
    vid             VID field
    <cr>
(config)# access-list ace 1
```

Example 2: Display specific ACE 1 configs:

```
(config)# access-list ace ?
    <1-512>    ACE ID
    update     Update an existing ACE
(config)# access-list ace 1 ?
    action          Access list action
    dmac-type       The type of destination MAC address
    frame-type      Frame type
    ingress         Ingress
    logging         Logging frame information. Note: The logging feature only
                    works when the packet length is less than 1518 (without
                    VLAN tags) and the System Log memory size and logging rate
                    is limited.
    next            insert the current ACE before the next ACE ID
    policy          Policy
    rate-limiter    Rate limiter
    redirect        Redirect frame to specific port
    shutdown        Shutdown incoming port. The shutdown feature only works
                    when the packet length is less than 1518 (without VLAN
                    tags).
    tag-priority    Tag priority
    vid             VID field
    <cr>
(config)# access-list ace 1 action ?
    deny      Deny
    permit    Permit
(config)# access-list ace 1 action permit ?
    dmac-type       The type of destination MAC address
    frame-type      Frame type
    ingress         Ingress
    logging         Logging frame information. Note: The logging feature only
                    works when the packet length is less than 1518 (without
                    VLAN tags) and the System Log memory size and logging rate
                    is limited.
    next            insert the current ACE before the next ACE ID
    policy          Policy
    rate-limiter    Rate limiter
    redirect        Redirect frame to specific port
    shutdown        Shutdown incoming port. The shutdown feature only works
                    when the packet length is less than 1518 (without VLAN
                    tags).
    tag-priority    Tag priority
    vid             VID field
    <cr>
(config)# access-list ace 1 action permit dmac-type ?
    any          Don't-care the type of destination MAC address
    broadcast    Broadcast destination MAC address
    multicast    Multicast destination MAC address
    unicast      Unicast destination MAC address
(config)# access-list ace 1 action permit dmac-type any ?
    frame-type      Frame type
    ingress         Ingress
```

```
    logging         Logging frame information. Note: The logging feature only
                    works when the packet length is less than 1518 (without
                    VLAN tags) and the System Log memory size and logging rate
                    is limited.
    next            insert the current ACE before the next ACE ID
    policy          Policy
    rate-limiter    Rate limiter
    redirect        Redirect frame to specific port
    shutdown        Shutdown incoming port. The shutdown feature only works
                    when the packet length is less than 1518 (without VLAN
                    tags).
    tag-priority    Tag priority
    vid             VID field
    <cr>
(config)# access-list ace 1 action permit dmac-type any frame-type ?
    any          Don't-care the frame type
    arp          Frame type of ARP
    etype        Frame type of etype
    ipv4         Frame type of IPv4
    ipv4-icmp    Frame type of IPv4 ICMP
    ipv4-tcp     Frame type of IPv4 TCP
    ipv4-udp     Frame type of IPv4 TCP
    ipv6         Frame type of IPv6
    ipv6-icmp    Frame type of IPv6 ICMP
    ipv6-tcp     Frame type of IPv6 TCP
    ipv6-udp     Frame type of IPv6 UDP
(config)# access-list ace 1 action permit dmac-type any frame-type etype ?
    dmac            Destination MAC address field
    etype-value     Etype value
    ingress         Ingress
    logging         Logging frame information. Note: The logging feature only
                    works when the packet length is less than 1518 (without
                    VLAN tags) and the System Log memory size and logging rate
                    is limited.
    next            insert the current ACE before the next ACE ID
    policy          Policy
    rate-limiter    Rate limiter
    redirect        Redirect frame to specific port
    shutdown        Shutdown incoming port. The shutdown feature only works
                    when the packet length is less than 1518 (without VLAN
                    tags).
    smac            Source MAC address field
    tag-priority    Tag priority
    vid             VID field
    <cr>
(config)# $t ace 1 action permit dmac-type any frame-type etype dmac ?
(config)# access-list ace 1 action permit dmac-type any evc-policer ?
    <EvcPolicerId : 1-256>    EVC policer ID
    disable                   Disable evc-policer
(config)# $t ace 1 action permit dmac-type any evc-policer 1 frame-type ?
    any          Don't-care the frame type
    arp          Frame type of ARP
    etype        Frame type of etype
```

```
    ipv4         Frame type of IPv4
    ipv4-icmp    Frame type of IPv4 ICMP
    ipv4-tcp     Frame type of IPv4 TCP
    ipv4-udp     Frame type of IPv4 TCP
    ipv6         Frame type of IPv6
    ipv6-icmp    Frame type of IPv6 ICMP
    ipv6-tcp     Frame type of IPv6 TCP
    ipv6-udp     Frame type of IPv6 UDP
(config)# $ion permit dmac-type any evc-policer 1 frame-type etype dmac ?
    <DmacAddr : mac_addr>    The value of destination MAC address field
    any            Don't-care the value of destination MAC address field
(config)# $ evc-policer 1 frame-type etype dmac any ingress any logging ?
    disable         Disable logging
    mirror          Mirror frame to destination mirror port
    next            insert the current ACE before the next ACE ID
    policy          Policy
    rate-limiter    Rate limiter
    shutdown      Shutdown incoming port. The shutdown feature only works
                    when the packet length is less than 1518 (without VLAN tags).
    tag             Tag
    tag-priority    Tag priority
    vid             VID field
    <cr>
(config)# $licer 1 frame-type etype dmac any ingress any logging mirror ?
    disable         Disable mirror
    next            insert the current ACE before the next ACE ID
    policy          Policy
    rate-limiter    Rate limiter
    shutdown        Shutdown incoming port. The shutdown feature only works
                    when the packet length is less than 1518 (without VLAN tags).
    tag             Tag
    tag-priority    Tag priority
    vid             VID field
    <cr>

(config)# $licer 1 frame-type etype dmac any ingress any logging mirror tag ?
    any         Don't-care tagged or untagged
    tagged      Tagged
    untagged    Untagged
(config)# $-type etype dmac any ingress any logging mirror tag any next ?
    <AceId : 1-256>    The next ID
    last               Place the current ACE to the end of access list
(config)# $pe dmac any ingress any logging mirror tag any next 2 policy ?
    <PolicyId : 0-255>    Policy ID
(config)# $any next 2 policy 1 policy-bitmask 9 rate-limiter 1 shutdown ?
    disable         Disable shutdown
    tag-priority    Tag priority
    vid             VID field
    <cr>
(config)# $olicy-bitmask 9 rate-limiter 1 shutdown disable tag-priority ?
    0-1                   The range of tag priority
    0-3                   The range of tag priority
    2-3                   The range of tag priority
```

```
    4-5                   The range of tag priority
    4-7                   The range of tag priority
    6-7                   The range of tag priority
    <TagPriority : 0-7>   The value of tag priority
    any                   Don't-care the value of tag priority field
(config)# $bitmask 9 rate-limiter 1 shutdown disable tag-priority 6 vid ?
    <Vid : 0-4095>    The value of VID field
    any               Don't-care the value of VID field
(config)# $bitmask 9 rate-limiter 1 shutdown disable tag-priority 6 vid any ?
    <cr>
(config)# $bitmask 9 rate-limiter 1 shutdown disable tag-priority 6 vid any
% The ACL rate limiter and EVC policer can not both be enabled.
(config)#
```

Command: Configure Access List Rate Limiter

Syntax: **access-list rate-limiter** [<rate_limiter_list>] { pps <pps_rate> | 10pps <pps10_rate> | 100pps <pps100_rate> | 25kbps <kpbs25_rate> | 100kbps <kpbs100_rate> }

Description: Configure access list rate limiter parameters. The rate range is **0**-**131071** in pps. The valid rate is **0** - **99**, **100**, **200**, **300**, ..., **1092000** in pps or **0**, **100**, **200**, **300**, ..., **1000000** in kbps. The valid unit values are **pps** (packets per second) and **kbps** (Kbits per second).

Mode: (config)#

Example:

```
(config)# access-list rate-limiter ?
    <1~16>    Rate limiter ID
    pps       Packets per second
(config)# access-list rate?
    rate-limiter    Rate limiter
(config)# access-list rate ?
    <1~16>    Rate limiter ID
    pps       Packets per second
(config)# access-list rate-limiter ?
    <1~16>    Rate limiter ID
    pps       Packets per second
(config)# access-list rate-limiter 1 ?
    pps    Packets per second
(config)# access-list rate-limiter 1 pps ?
    <0-131071>    Rate value
(config)# access-list rate-limiter 1 pps 90000 ?
    <cr>
(config)# access-list rate-limiter 1 pps 90000
(config)#
```

Command: Configure Aggregation

Syntax: **aggregation mode** { [smac] [dmac] [ip] [port] }*1
Description: Configure aggregation mode in terms of DMAC, SMAC, IP address, and port number. Frames destined for a LAG are sent on only one of the LAGs member ports. The member port on which a frame is forwarded is determined by a 4-bit aggregation code (AC) that is calculated for the frame. The aggregation code ensures that frames belonging to the same frame flow (e.g., a TCP connection) are always forwarded on the same LAG member port. For that reason, reordering of frames within a flow is not possible. The AC is based on the following information: **1**. SMAC (Source MAC address), **2**. DMAC (Destination MAC address), **3**. Source and Destination IPv4 address, **4**. Source and Destination TCP/UDP ports for IPv4 packets, **5**. Source and Destination TCP/UDP ports for IPv6 packets, and **6**.IPv6 Flow Label. For best traffic distribution among LAG member ports, enable all six contributions to the AC. Each LAG can consist of up to 16 member ports. Any quantity of LAGs may be configured for the S4224 (only limited by the number of device ports). To configure a proper traffic distribution, the ports within a LAG must use the same link speed.
Mode: (config)#
Example: Configure aggregation mode and show resulting config:

```
(config)# aggregation ?
    mode    Traffic distribution mode
(config)# aggreg mode ?
    dmac    Destination MAC affects the distribution
    ip      IP address affects the distribution
    port    IP port affects the distribution
    smac    Source MAC affects the distribution
    <cr>
(config)# aggreg mode smac ?
    dmac    Destination MAC affects the distribution
    ip      IP address affects the distribution
    port    IP port affects the distribution
    <cr>
(config)# aggreg mode dmac ?
    ip      IP address affects the distribution
    port    IP port affects the distribution
    smac    Source MAC affects the distribution
    <cr>
(config)# aggreg mode dmac ip ?
    port    IP port affects the distribution
    smac    Source MAC affects the distribution
    <cr>
(config)# aggreg mode dmac port ?
    ip      IP address affects the distribution
    smac    Source MAC affects the distribution
    <cr>
(config)# aggregation mode dmac?
aggregation mode { [ smac ] [ dmac ] [ ip ] [ port ] }*1
(config)# aggregation mode dmac
(config)# aggregation mode smac
(config)# aggregation mode ip
(config)# end
# show aggregation mode
Aggregation Mode:

SMAC  : Enabled
DMAC  : Enabled
IP    : Enabled
Port  : Enabled
# show aggregation
#
```

Command: Configure Banner

Syntax: **config banner**
Description: Configure login banner parameters.
Mode: (config)#
Example:

```
(config)# banner ?
    <line>    c banner-text c, where 'c' is a delimiting character
    exec      Set EXEC process creation banner
    login     Set login banner
    motd      Set Message of the Day banner
(config)# banner?
    banner    Define a login banner
(config)# banner??
banner [ motd ] <banner>
banner exec <banner>
banner login <banner>
(config)# banner
(config)# banner login ?
    LINE    c banner-text c, where 'c' is a delimiting character
(config)# banner exec ?
    LINE    c banner-text c, where 'c' is a delimiting character
(config)# banner motd ?
    LINE    c banner-text c, where 'c' is a delimiting character
(config)#
```

Command: Configure ToD Clock

Syntax: **config clock**
Description: Configure the time-of-day clock in terms of the timezone and DST (daylight savings time). The parameters are:

clock summer-time <word16> recurring [<start_week_var> <start_day_var> <start_month_var> <start_hour_var> <end_week_var> <end_day_var> <end_month_var> <end_hour_var> [<offset_var>]]

clock timezone <word_var> <hour_var> [<minute_var> [<subtype_var>]]

Mode: (config)#
Example: Examine the time of day clock commands.

```
(config)# clock ?
    summer-time  Configure summer (daylight savings) time where:
    timezone     Configure time zone where WORD = the name of the time zone (the
                 Hours offset from UTC - from <-23-23>).
(config)# clock?
    clock    Configure time-of-day clock
(config)# clock??
clock summer-time <word16> date [ <start_month_var> <start_date_var> <start_year
_var> <start_hour_var> <end_month_var> <end_date_var> <end_year_var> <end_hour_v
ar> [ <offset_var> ] ]
clock summer-time <word16> recurring [ <start_week_var> <start_day_var> <start_m
onth_var> <start_hour_var> <end_week_var> <end_day_var> <end_month_var> <end_hou
r_var> [ <offset_var> ] ]
clock timezone <word_var> <hour_var> [ <minute_var> [ <subtype_var> ] ]
(config)# clock
```

Command: Configure DDMI

Syntax: **config ddmi**

Description: Configure the DDMI Information. DDMI (Digital Diagnostics Monitoring Interface) provides an enhanced digital diagnostic monitoring interface for optical transceivers which allows real time access to device operating parameters.

Mode: (config)#

Example: Enable and disable DDMI and use the show command to display the resulting state:

```
(config)# ddmi?
    ddmi    DDMI Information
    <cr>
(config)# ddmi ?
    <cr>
(config)# ddmi
(config)#
(config)# no ddmi
(config)# end
# show ddmi ?
    <cr>
# show ddmi
Current mode: Disabled
#
# show ddmi
Current mode: Enabled
# con ter
(config)# ddmi ?
    <cr>
(config)# ddmi
(config)# do show ddmi
Current mode: Enabled
(config)# no ddmi
(config)# do show ddmi
Current mode: Disabled
(config)#
```

Command: Configure Default Access List Rate Limiter

Syntax: **config default access-list rate-limiter** [<1-16>]
Description: Configure the access-list rate-limiter to its default settings.
Mode: (config)
Example:

```
(config)# default?
    default    Set a command to its defaults
(config)# default ?
    access-list    Access list
(config)# default ?
default access-list rate-limiter [ <1~16> ]
(config)# default access-list rate-limiter
(config)#end
# show access-list rate-limiter
Switch access-list rate limiter ID 1 is 0 pps
Switch access-list rate limiter ID 2 is 1 pps
Switch access-list rate limiter ID 3 is 1 pps
Switch access-list rate limiter ID 4 is 1 pps
Switch access-list rate limiter ID 5 is 1 pps
Switch access-list rate limiter ID 6 is 1 pps
Switch access-list rate limiter ID 7 is 1 pps
Switch access-list rate limiter ID 8 is 1 pps
Switch access-list rate limiter ID 9 is 1 pps
Switch access-list rate limiter ID 10 is 1 pps
Switch access-list rate limiter ID 11 is 1 pps
Switch access-list rate limiter ID 12 is 1 pps
Switch access-list rate limiter ID 13 is 1 pps
Switch access-list rate limiter ID 14 is 1 pps
Switch access-list rate limiter ID 15 is 1 pps
Switch access-list rate limiter ID 16 is 1 pps
```

Command: Configure Do

Syntax: **config do**
Description: To run exec commands in config mode. Note that no ‘do’ prefix is needed in Exec mode.
Mode: (config)
Example:

```
(config)# do ?
LINE
(config)# do ?
    LINE    Exec Command
(config)# do
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# do show ip interface brief
Vlan Address Method Status
---- ------------------- -------- ------
 1 172.16.1.15/24 DHCP UP
(config-if-vlan)# end

! When in Exec, no ‘do’ prefix is needed:
# show ip interface brief
Vlan   Address                    Method  Status
----   -------------------  --------      ------
  1    172.16.1.15/24               DHCP          UP
```

Command: Configure Dot1x NAC

Syntax: **config dot1x**

Description: Configure the IEEE Standard for port-based Network Access Control. The commands are:

dot1x authentication timer inactivity <v_10_to_100000>
dot1x authentication timer re-authenticate <v_1_to_3600>
dot1x feature { [guest-vlan] [radius-qos] [radius-vlan] }*1. Globally enables/disables a dot1x feature functionality.
dot1x guest-vlan <value>
dot1x guest-vlan supplicant
dot1x max-reauth-req <value>. The number of times a Request Identity EAPOL frame is sent without response before considering entering the Guest VLAN.
dot1x re-authentication Set Re-authentication state.
dot1x system-auth-control Set the global NAS state.
dot1x timeout quiet-period <v_10_to_1000000>
dot1x timeout tx-period <v_1_to_65535>

Mode: (config)

Example 1: Configure the various NAC functions available.

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

Example 2: Configure NAC authentication.

```
(config)# dot1x authentication ?
    timer    timer
(config)# dot1x authentication timer ?
    inactivity          Time in seconds between check for activity on
                        successfully authenticated MAC addresses.
    re-authenticate     The period between re-authentication attempts in seconds
(config)# dot1x authentication timer inactivity ?
    <10-1000000>    seconds
(config)# dot1x authentication timer inactivity 50000 ?
    <cr>
(config)# dot1x authentication timer inactivity 50000
```

Example 3: Configure NAC features set.

```
(config)# dot1x feature ?
    guest-vlan     Globally enables/disables state of guest-vlan
    radius-qos     Globally enables/disables state of RADIUS-assigned QoS.
    radius-vlan    Globally enables/disables state of RADIUS-assigned VLAN.
(config)# dot1x feature guest-vlan ?
    radius-qos     Globally enables/disables state of RADIUS-assigned QoS.
    radius-vlan    Globally enables/disables state of RADIUS-assigned VLAN.
    <cr>
(config)# dot1x feature guest-vlan
(config)# dot1x feature radius-qos ?
    guest-vlan     Globally enables/disables state of guest-vlan
    radius-vlan    Globally enables/disables state of RADIUS-assigned VLAN.
    <cr>
(config)# dot1x feature radius-vlan
```

Example 4: Configure NAC Max Re-authentication.

```
(config)# dot1x max-reauth-req ?
    <1-255>    number of times
(config)# dot1x max-reauth-req 55 ?
    <cr>
(config)# dot1x max-reauth-req 55
(config)# dot1x re-authentication ?
    <cr>
(config)# dot1x re-authentication
```

Example 5: Configure NAC System Authentication.

```
(config)# dot1x system-auth-control ?
    <cr>
(config)# dot1x system-auth-control
```

Example 6: Configure NAC System Timeout and Quiet Period.

```
(config)# dot1x timeout ?
    quiet-period    Time in seconds before a MAC-address that failed
                    authentication gets a new authentication chance.
    tx-period       the time between EAPOL retransmissions.
(config)# dot1x timeout quiet-period ?
    <10-1000000>    seconds
(config)# dot1x timeout quiet-period 100 ?
    <cr>
(config)# dot1x timeout quiet-period 100
(config)# dot1x timeout tx-period ?
    <1-65535>    seconds
(config)# dot1x timeout tx-period 900 ?
    <cr>
(config)# dot1x timeout tx-period 900
(config)#
```

Command: Configure Password Parameters

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

Description: Modify password parameters. You can set privilege attributes to each command. A user cannot access or execute a command unless the logged in user has sufficient priveleges assigned. (Not to be confused with User Exec mode and Privileged EXEC mode priveleges.)

Mode: (config)

Example:

```
(config)# enable ?
    password    Assign the privileged level clear password, where:
    <word32>    The UNENCRYPTED (cleartext) password
    level       Set exec level password
    secret      Assign the privileged level secret, where:
           WORD     The UNENCRYPTED (cleartext) password.
(config)# enable secret ?
    0    Specifies an UNENCRYPTED password will follow
    5    Specifies an ENCRYPTED secret will follow
(config)# enable secret 0 ?
    <word32>    Password
    level       Set exec level password
(config)# enable secret ?
    0    Specifies an UNENCRYPTED password will follow
    5    Specifies an ENCRYPTED secret will follow
(config)# enable secret 5 ?
    <word32>    Password
    level       Set exec level password
 (config)# enable secret 5 level ?
    <1-15>    Level number
(config)# enable secret 5 level
```

Command: End Configuration Mode

Syntax: **end**

Description: Go back to EXEC mode (from config mode).

Mode: (config)

Example:

```
(config)# end ?
    <cr>
(config)# end
#
```

Command: Configure EPS

Syntax: **config eps**

Description: Configure Ethernet Protection Switching (EPS) parameters. Linear Protection is implemented for maintaining connectivity via alternate path in case the current data path fails. Two or more parallel instances are configured between ports of a unit pair. Two of the paths are configured into an Ethernet Protection switching group as a pair of Working-Protecting instances. By default, the designated Working instance is used for data communication. In case of a failure of the Working instance, a Protection switch is executed and the Protecting instance then bears the traffic.

The implementation uses mechanisms defined in Ethernet OAM Specifications (ITU-T.Y.1731) for checking path health. OAM MEPs are configured on instances configured in the Protection Setup between peer units.

Protection Groups can be configured to support revertive or non-revertive mode (i.e., when the Working instance has been restored, whether there should be a Protection switch to use the Working instance again or whether to continue using the Protecting instance).

Time to react to instance faults and also to hold for some time between switches can also be configured to increase the efficiency of Protection switching and avoiding intermittent/unstable instance conditions.

You must disable Spanning Tree for CIST ports (1 and 2) on devices at both ends.
EPS requires that MEP config is done (the EPS config builds on the MEP configuration).
EPS requires Working (Primary) and Protection (Secondary) links established. These links are responsible for APS frame transmission. APS must be enabled on the associated MEPs. Therefore MEPs must be created for Working and Protection links prior to configuring EPS.
Different protection schemes (1+1, 1:1, 1:N) can be configured as detailed in the sections below.

eps <inst> **1plus1** { bidirectional | { unidirectional [aps] } }
eps <inst> **command** { lockout | forced | manualp | manualw | exercise | freeze |lockoutlocal }
eps <inst> **domain** { port | evc } **architecture** { 1plus1 | 1for1 } **work-flow** { <flow_w> | <port_type> <port_w> }
protect-flow { <flow_p> | <port_type> <port_p> }
eps <inst> **holdoff** <hold>
eps <inst> **mep-work** <mep_w> mep-protect <mep_p> mep-aps <mep_aps>
eps <inst> **revertive** { 10s | 30s | 5m | 6m | 7m | 8m | 9m | 10m | 11m | 12m }
eps <inst> **1plus1** { bidirectional | { unidirectional [aps] } }
eps <inst> **command** { lockout | forced | manualp | manualw | exercise | freeze |lockoutlocal }
eps <inst> **domain** { port | tunnel-tp | pw } **architecture** { 1plus1 | 1for1 } **work-flow** { <flow_w> | <port_type> <port_w> } protect-flow { <flow_p> | <port_type><port_p> }
eps <inst> **holdoff** <hold>
eps <inst> **mep-work** <mep_w> mep-protect <mep_p> mep-aps <mep_aps>
eps <inst> **revertive** { 10s | 30s | 5m | 6m | 7m | 8m | 9m | 10m | 11m | 12m | {wtr-value <wtr_value> } }

Mode: (config)

Example 1: Display the EPS command options.

```
(config)# eps?
    eps    Ethernet Protection Switching.
(config)# eps ?
    <Inst : uint>    The EPS instance number.
(config)# eps 1 ?
    1plus1       EPS 1+1 architecture.
    command      EPS command.
    domain       The domain of the EPS.
    holdoff      Hold off timer.
    mep-work     Working MEP instance.
    revertive    Revertive EPS.
```

Example 2: Display the EPS 1 + 1 options:

```
(config)# eps 2 1plus1 ?
    bidirectional     EPS 1+1 bidirectional protection type.
    unidirectional    EPS 1+1 unidirectional protection type.
(config)# eps 2 1plus1 bidirectional ?
    <cr>
```

Example 3: Display the EPS Command options:

```
(config)# eps 2 command ?
    exercise        Exercise signal.
    forced          Force switch normal traffic to protection.
    freeze          Local Freeze of EPS.
    lockout         Lockout of protection.
    lockoutlocal    Local lockout of EPS.
    manualp         Manual switch normal traffic to protection.
    manualw         Manual switch normal traffic to working.
(config)# eps 2 command exercise ?
    <cr>(config)# eps 2 command forced ?
    <cr>
(config)# eps 2 command freeze ?
    <cr>
(config)# eps 2 command lockout ?
    <cr>
(config)# eps 2 command lockoutlocal ?
    <cr>
(config)# eps 2 command manualp ?
    <cr>
(config)# eps 2 command manualp?
    manualp    Manual switch normal traffic to protection.
    <cr>
(config)# eps 2 command manualw ?
    <cr>
(config)# eps 2 command exercise?
    exercise    Exercise signal.
    <cr>
(config)# eps 2 command forced?
    forced    Force switch normal traffic to protection.
    <cr>
(config)# eps 2 command freeze?
    freeze    Local Freeze of EPS.
    <cr>
(config)# eps 2 command lockout?
    lockout         Lockout of protection.
    lockoutlocal    Local lockout of EPS.
    <cr>
(config)# eps 2 command manual?
    manualp    Manual switch normal traffic to protection.
    manualw    Manual switch normal traffic to working.
(config)# eps 2 command manual
```

Example 4: Display the EPS Domain options:

```
(config)# eps 1 domain?
    domain    The domain of the EPS.
(config)# eps 1 domain ?
    evc     This EPS is protecting in the EVC domain.
    port    This EPS is protecting in the Port domain.
(config)# eps 1 domain evc ?
    architecture    The EPS architecture.
(config)# eps 1 domain evc architecture ?
    1for1     The architecture is 1 for 1.
    1for1     The architecture is 1 for 1.
(config)# eps 1 domain evc architecture 1for1 ?
    work-flow    The working flow instance that the EPS is related to.
(config)# eps 1 domain evc architecture 1for1 work-flow ?
    GigabitEthernet       1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
    <FlowW : uint>        The working flow instance number when not in the port domain.
(config)# eps 1 domain evc architecture 1for1 work-flow 1 ?
    protect-flow    The protecting flow instance that the EPS is related to.
(config)# eps 1 domain evc architecture 1for1 work-flow 1 protect-flow ?
    GigabitEthernet       1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
    <FlowP : uint>        The protecting flow instance number when not in the port domain.
(config)# eps 1 domain evc architecture 1for1 work-flow 1 protect-flow 1 ?
    <cr>
(config)# eps 1 domain evc architecture 1for1 work-flow 1 protect-flow 1
(config)#
```

Example 5: Display the EPS Holdoff and Working MEP options:

```
(config)# eps 1 holdoff ?
    <Hold : uint>    The hold off timer value in 100 ms. Max 10 sec.
(config)# eps 1 holdoff 1 ?
    <cr>
(config)# eps 1 mep-work ?
    <MepW : uint>    Working MEP instance number.
(config)# eps 1 mep-work 2 ?
    mep-protect    Protecting MEP instance.
(config)# eps 1 mep-work 2 mep-protect ?
    <MepP : uint>    Protecting MEP instance number.
(config)# eps 1 mep-work 2 mep-protect 3 ?
    mep-aps    APS MEP instance.
(config)# eps 1 mep-work 2 mep-protect 3 mep-aps ?
    <MepAps : uint>    APS MEP instance number.
(config)# eps 1 mep-work 2 mep-protect 3 mep-aps 1 ?
    <cr>
(config)# eps 1 mep-work 2 mep-protect 3 mep-aps 1
(config)#
```

Example 5: Display the EPS Revertive options:

```
(config)# eps 1 revertive ?
    10m    WTR is 10 min.
    10s    WTR is 10 sec.
    11m    WTR is 11 min.
    12m    WTR is 12 min.
    30s    WTR is 30 sec.
    5m     WTR is 5 min.
    6m     WTR is 6 min.
    7m     WTR is 7 min.
    8m     WTR is 8 min.
    9m     WTR is 9 min.
(config)# eps 1 revertive 10 ?
                          ^
% Ambiguous word detected at '^' marker.

(config)# eps 1 revertive 10s ?
    <cr>
(config)# eps 1 revertive 10s
(config)#
```

EPS (Port Protection) Parameters

An Ethernet Protection switching Group can be created by configuring these parameters:

Configurable Parameter	Valid Range	Default
EPS Id	1-100	1
Domain	Port/EVC	Port
Architecture	1:1/1+1	1+1
Working Flow	Valid port range / Flow Id	1
Protecting Flow	Valid port range / Flow Id	1
Working SF Reporting MEP	Valid MEP Id	1
Protecting SF Reporting MEP	Valid MEP Id	1
APS PDU handling MEP	Valid MEP Id	1
Instance Configuration		
Protection Type (only for 1+1)	Uni/Bidirectional	Unidirectional
APS (only for 1+1)	Enable/Disable	Disabled
Revertive	Yes/No	No
WTR Time	Disabled / 10sec / 30sec / 5min / 6min / 7min / 8min / 9min / 10min / 11min / 12min	Disabled
Hold Off Time	Disabled / 100ms- 900ms (incr 100ms) / 1sec - 10sec (incr1 sec)	Disabled
Instance command	None / Clear / LockOut / ForcedSwitch / Manual Switch P / Manual SwitchW / Exercise / Freeze / Lock Out Local	None

1+1 Port Protection

Two ports on a unit are paired with two ports on a Peer-Unit to create a Working-Protecting pair between the units. After the initialization of Protection Group, Both links are active and transmit data. When a link-failure is detected, the Protecting Link is used to continue data transmission.

1:1 Port Protection
Two ports on a Unit a paired with two ports on a Peer-Unit to create a Working-Protecting pair between the units. After the initialization of Protection Group only the Working Flow is active and both end points of the Protecting Flow are blocked for data transmission. When a link failure is detected on the Working Link, a Protection switch is initiated and the Protecting Link will now be used for active data exchange.

1:N Port Protection
The sections above list a strict 1:1 redundancy. However, there are two points to consider when setting up redundancy:

- Strict pair redundancy reduces the actual number of usable ports to n/2 which may not be the best use of available resources.
- The probability of all or most links failing at the same time is very low.

Considering the above, a 1:N Port Protection scheme is also possible.

Multiple 1:1 protection groups are configured but the same Protecting Link is chosen in all the groups as a fall-back for the Working Link. Assuming that any of the Working Link fails, a Protection switch to this Protecting Link can be made and traffic can be restored.

Once the faulty Working Link is restored, Automatic (Revertive)/Manual Protection switch can be done to make the Protection Link available to other Groups.

Note that if one of the Working Link is down and a Protection switch is executed, all the other Working Links (with same Protection Link as back-up) go into an administrative hold-mode. This means that if there is a Link Failure in one of these links, there will be no switchover to a Protecting Link.

Command: Config ERPS

Syntax: **erps**

Description: Configure Ethernet Ring Protection Switching (ERPS) parameters. Note that the ***erps*** command is also available in Exec mode. **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 Config Commands" on page 78.

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 S4224 implements the ITU G.8032 standard for ERPS, which uses the APS automatic protection protocol for protection in ring and interconnected ring topology. The S4224 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.

Mode: (config)

Example: Display the various ERPS functions and parameters.

```
(config)# erps?
(config)# erps ?
    1-64    ERPS group number
(config)# erps?
    erps    Ethernet Ring Protection Switching
(config)# erps??
erps <group> command { force | manual | clear } { port0 | port1 }
erps <group> guard <guard_time_ms>
erps <group> holdoff <holdoff_time_ms>
erps <group> major port0 interface <port_type> <port0> port1 interface <port_type> <port1> [
interconnect ]
erps <group> mep port0 sf <p0_sf> aps <p0_aps> port1 sf <p1_sf> aps <p1_aps>
erps <group> revertive <wtr_time_minutes>
erps <group> rpl { owner | neighbor } { port0 | port1 }
erps <group> sub port0 interface <port_type> <port0> { { port1 interface <port_type> <port1>
} | { interconnect <major_ring_id> [ virtual-channel ] } }
erps <group> topology-change propagate
erps <group> version { 1 | 2 }
erps <group> vlan { none | [ add | remove ] <vlans> }
(config)# erps
```

Example 2: Configure ERPS 1 as Major ring and show the resulting configuration.

```
(config)# erps ?
    1-64    ERPS group number
(config)# erps 1 ?
    command             Administrative Command
    guard               Guard
    holdoff             Holdoff
    major               Major ring
    mep                 MEP
    revertive           Revertive
    rpl                 Ring Protection Link
    sub                 Sub-ring
    topology-change     Topology Change
    version             Version
    vlan                VLAN
(config)# erps 1 major ?
    port0    ERPS Port 0 interface
(config)# erps 1 major port0 ?
    interface    Ethernet interface
(config)# erps 1 major port0 interface ?
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
 (config)# erps 1 major port0 interface g ?
    PORT_ID    Port ID in 1/1-6
(config)# erps 1 major port0 interface g 1/1 ?
    port1    ERPS Port 1 interface
(config)# erps 1 major port0 interface g 1/1 port1 ?
    interface    Ethernet interface
(config)# erps 1 major port0 interface g 1/1 port1 interface ?
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
(config)# erps 1 major port0 interface g 1/1 port1 interface g ?
    PORT_ID    Port ID in 1/1-6
(config)# erps 1 major port0 interface g 1/1 port1 interface g 1/1
% ERPS group 1: Port 0 and port 1 are the same
(config)# erps 1 major port0 interface g 1/1 port1 interface g 1/2
(config)# end
# show erps ?
    1~64          Zero or more ERPS group numbers
    |             Output modifiers
    detail        Show detailed information
    statistics    Show statistics
    <cr>
# show erps 1
(L=Link Up/Down; B=Blocked/Unblocked)      Maj RPL  RPL   RPL  FSM   R-APS
Gr Typ V Rev Port 0     L B Port 1     L B Grp Role Port  Blck State TX RX FOP
--+---+-+---+----------+-+-+----------+-+-+---+----+-----+----+-----+--+--+---
 1 Maj 2 Rev Gi 1/1     U B Gi 1/2     U B -   -    -     -    NONE  N     N
#
```

Example 3: Configure ERPS 2 as a Sub-Ring and show the resulting configuration.

```
(config)# erps 2 sub ?
    port0    ERPS Port 0 interface
(config)# erps 2 sub port0 ?
    interface    Ethernet interface
(config)# erps 2 sub port0 interface ?
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
(config)# erps 2 sub port0 interface 10GigabitEthernet ?
    PORT_ID    Port ID in 1/1-2
(config)# erps 2 sub port0 interface 10GigabitEthernet 1/2 ?
```

```
    interconnect    Sub-ring is interconnected
    port1           ERPS Port 1 interface
(config)# $ps 2 sub port0 interface 10GigabitEthernet 1/2 interconnect ?
    1-64    Major ring group number
(config)# $ps 2 sub port0 interface 10GigabitEthernet 1/2 interconnect 1 ?
    virtual-channel    Enable virtual channel for sub-ring
    <cr>
(config)# $erface 10GigabitEthernet 1/2 interconnect 1 virtual-channel ?
    <cr>
(config)# $erface 10GigabitEthernet 1/2 interconnect 1 virtual-channel 1

erps 2 sub port0 interface 10GigabitEthernet 1/2 interconnect 1 virtual-channe
l 1
  ^
% Invalid word detected at '^' marker.

(config)# $ 10GigabitEthernet 1/2 interconnect 1 virtual-channel
(config)# end
# show erps
(L=Link Up/Down; B=Blocked/Unblocked)      Maj RPL  RPL   RPL  FSM   R-APS
Gr Typ V Rev Port 0     L B Port 1     L B Grp Role Port  Blck State TX RX FOP
--+---+-+---+----------+-+-+----------+-+-+---+----+-----+----+-----+--+--+---
 1 Maj 2 Rev Gi 1/1     U B Gi 1/2     U B -   -    -     -    NONE  N     N
 2 S-I 2 Rev 2.5G 1/2   U B -          U U 1   -    -     -    NONE  N     N
#
```

Example 4: Configure ERPS 1 Guard time, Holdoff time,Revertive, RPL, Topology, and VLAN parameters, and then display the resulting configuration.

```
(config)# erps 1 guard ?
    10-2000    Guard time in ms
(config)# erps 1 guard 300 ?
    <cr>
(config)# erps 1 guard 300
(config)# erps 1 holdoff ?
    0-10000    Holdoff time in ms
(config)# erps 1 holdoff 2050
% Holdoff time rounded to 2000 ms
(config)# erps 1 revertive ?
    1-12    Wait-to-restore time in minutes
(config)# erps 1 revertive 2 ?
    <cr>
(config)# erps 1 revertive 2
(config)# erps 1 rpl ?
    neighbor    Neighbor role
    owner       Owner role
(config)# erps 1 rpl owner ?
    port0    ERPS Port 0 interface
    port1    ERPS Port 1 interface
 (config)# erps 1 rpl owner port0
(config)# erps 1 topology-change ?
    propagate    Propagate
(config)# erps 1 topology-change propagate ?
    <cr>
(config)# erps 1 topology-change propagate
 (config)# erps 1 vlan ?
    <vlan_list>    List of VLANs
    add            Add to set of included VLANs
    none           Do not include any VLANs
    remove         Remove from set of included VLANs
(config)# erps 1 vlan add ?
    <vlan_list>    List of VLANs
```

```
(config)# erps 1 vlan add 1
(config)# end
# show erps
(L=Link Up/Down; B=Blocked/Unblocked)      Maj RPL  RPL   RPL  FSM   R-APS
Gr Typ V Rev Port 0     L B Port 1     L B Grp Role Port  Blck State TX RX FOP
--+---+-+---+----------+-+-+----------+-+-+---+----+-----+----+-----+--+--+---
 1 Maj 2 Rev Gi 1/1     U B Gi 1/2     U U -   Ownr Port0 Y    PEND  Y     N
 2 S-I 2 Rev 2.5G 1/2   U B -          U U 1   -    -     -    NONE  N     N
#
```

Command: ERPS Force/Manual/Clear

Syntax: **erps** <group> **command** { force | manual | clear } { port0 | port1 }

Description: Configure Ethernet Ring Protection Switching. A port can be administratively configured to be in either Manual switch or Forced switch state. The parameters are:

ERPS group number : 1-64

force : Forced Switch command forces a block on the ring port where the command is issued.

manual: : In the absence of a failure or FS, Manual Switch command forces a block on the ring port where the command is issued.

clear : The Clear command is used for clearing an active local administrative command (e.g., Forced Switch or Manual Switch).

Mode: (config)#

Example 1: Display the functions / parameters, configure an instance, and show the resulting config.

```
(config)# erps 1 command ?
    clear     Clear command
    force     Force command
    manual    Manual command
(config)# erps 1 command clear ?
    port0    ERPS Port 0 interface
    port1    ERPS Port 1 interface
(config)# erps 1 command clear port0 ?
    <cr>
(config)# erps 1 command clear port1 ?
    <cr>
 (config)# erps 1 command clear port1
% ERPS group 1: Generic error occurred
(config)# erps 1 command clear port0
% ERPS group 1: Generic error occurred
(config)#
(config)# erps 1 command clear port0
(config)#
```

Messages: *% ERPS group 1: Generic error occurred*

Ethernet Ring Protection

Ethernet rings can provide wide-area multipoint connectivity more economically due to their reduced number of links. Using a high capacity link such as SONET or SDH as the underlying Server layer, Local LANs communicate to remote networks in the Enterprise Network in real time over the larger ring topology. However, Ring protection mechanisms are required to prevent path failures in the topology while ensuring that no loops are created.

G.8032 Ring Protection

Ethernet Ring Protection is implemented per the requirements in ITU-T.G.8032. It uses the Continuity Check Message (CCM) and other OAM frame formats as defined in ITU-T.Y.1731 (specification for Ethernet OAM). It is capable of recovering multipoint connectivity in the event of a single ring-link or node failure.

To achieve the objectives of Ring Protection, the ETH layer connectivity of ring links is periodically monitored using CCM. Further, the Ring Protection mechanism communicates with the ETH layer and the Server layer for Signal Failure (SF) notifications to establish link state.

The implementation does not restrict the number of nodes that may form the Ethernet ring. However, from an operational perspective the maximum number of groups is limited to 64.

ERPS Parameters

ERPS instances can be created using the basic parameters below:

Configurable Parameter	Valid Range	Default
ERPS Id	1-64	1
Port 0 (East port)	Valid port range	1
Port 1 (West Port)	Valid port range	1
	Port 0 SF MEP 1-32	1
	Port 1 SF MEP 1-32	1
	Port 0 APS MEP 1-32	1
	Port 1 APS MEP 1-32	1
	Ring type Major/Sub	Major
Interconnected Node	Yes/No	No
Virtual Channel	Yes/No	No
Major Ring Id (Interconnected Sub ring)	0-99	0

Individual ERPS instances have following configurable parameters:

Configurable Parameter	Valid Range	Default
Instance Configuration		
Guard Time	10ms-2000ms, in steps of 10 ms	500 ms
WTR Time	1min, 5min - 12min	1 min
Hold Off Time	0ms - 10000ms, in steps of 100ms	0 ms
Version	v1/v2	v2
Revertive	Enable/Disable	Enable
VLAN Config		
VLAN ID	1-4094	N/A
RPL Configuration		
Role	None / RPL_Owner / RPL_Neighbour	None
Port	Port0 / Port1	None
Instance Command		
Command	None, Manual Switch, Forced Switch	None
Port	Port0 / Port1	None

Command: Configure EtherSAT (Service Activation Test)

Syntax: **ethersat**

Description: Configure the Ethersat (Service Activation Test) parameters.

collector : EtherSAT Collector [enable|disable]
loopback : TN Ethersat loopback
peerproto : EtherSAT PeerProto
profile : Ethersat profile
test : EtherSAT test

Mode: (config)#

Example 1: Show all of the EtherSAT parameters:

```
(config)# ethersat??
ethersat [ collector { enable | disable } ] [ peerproto { enable | disable } ]
ethersat loopback smac <smacaddr>
ethersat loopback state { active | inactive }
ethersat loopback testsideport { port ( <port_type> [ <port_list> ] ) }
ethersat loopback timeout <tout>
ethersat loopback vid { <vid> }
ethersat profile <pid> [ name <name> ] [ flratio <flr_ratio> ] [ linerate <linerate> ] [ sizemix <sizelist> ] [
ratedecstep <ratedecstep> ] [ steplength <steplen> ] [ yellowpcp <pcplist> ] [ yellowpcpmask <mask> ] [ clearpcp ] [
testmode {unidir | bidir | loopback } ] [ teststep { [ throughput ] [ latency ] [ flr ] [back-to-back ] [ all ] }*1 ] [
framefill { prbs | fixed <fixed_pattern> } ] [ dm-threshold <dmth> ] [ dmv-threshold <dmvth> ] { [ frmencaps { [ L2 { [
eth-test [ meglevel <meglevel1> ] ] | [ ceth-test { etype <ethtyp> [ meglevel <meglevel2> ] } ] | [ llc-snap { snap
<snap_list> sprot <snapproto> } ] } ] | [ L3 { udp | tcp } [ ip-header { sradr <sip> destadr <dip> dscp <dscp> ecn <ecn>
flags <ipflags> ttl <ttl> } ] { [ udp-header { udpsrcport <udpsrcport> udpdestport <udpdestport> } ] | [ tcp-header {
tcpsrcport <tcpsrcport> tcpdestport <tcpdestport> seqnum <seqnum> acknum <acknum> controlbits <controlbits> windowsize
<windowsize> }] } ] } ] }
ethersat profile new { <pid> } [ name <profname> ]
ethersat test new <testid> { [ testname <testname> ] } { profile <pid> } { cip <caddr> } { cinport <cinp> } { inport
<inp> } { inencaps-type { none | c-tag | s-tag | cs-tag | cc-tag } [ ivid <itvid> ] [ ipcp <inpcp> ] [ ovid <otvid> ] [
opcp <outpcp> ] } { egencaps-type { none | c-tag | s-tag | cs-tag | cc-tag } [ ivid <egitvid> ] [ ipcp <eginpcp> ] [ ovid
<egotvid> ] [ opcp <egoutpcp> ] }ethersat test results { testid <tid> } { all | throughput | latency | flr | b2b}
ethersat test { testid <tid> } [ testname <testname> ] [ delete ] [ start ] [ stop ] [ profile <pid> ] [ bandwidth {
policer-id <polid> } ] [ cir <cir> ] [ cbs<cbs> ] [ eir <eir> ] [ ebs <ebs> ] [ testmacaddr <macaddr> ] [ showconfig ] [
i
ngress [ inencaps-type { none | c-tag | s-tag | cs-tag | cc-tag } ] [ ivid <itvid> ] [ ipcp <inpcp> ] [ ovid <otvid> ] [
opcp <outpcp> ] ] [ egress [ egencaps-type { none | c-tag | s-tag | cs-tag | cc-tag } ] [ ivid <egitvid> ] [ ipcp
<eginpcp> ] [ ovid <egotvid> ] [ opcp <egoutpcp> ] ]
(config)# ethersat
```

Example 2: Configure the EtherSAT **collector** parameters:

```
(config)# ethersat collector ?
    disable    disable: Reject SA test requests from outside
    enable     enable : Accept SA test requests from outside
(config)# ethersat collector enable
Can't set ethersat flags
(config)# ethersat collector disable
Can't set ethersat flags
(config)#
```

Example 3: Configure the EtherSAT **loopback** parameters:

```
(config)# ethersat loopback ?
    smac            TN ethersat loopback SMAC address
    state           ethersat loopback State
    testsideport    ethersat loopback testsideport
    timeout         ethersat loopback timeout
    vid             Define ethersat loopback VLAN vid
(config)# ethersat loopback smac ?
    <mac_addr>    SMAC 48 bit MAC address: xx:xx:xx:xx:xx:xx
(config)# ethersat loopback state ?
```

```
    active      ethersat loopback active
    inactive    ethersat loopback inactive
(config)# ethersat loopback testsideport ?
    port    Set the loopback testsideport (number of ports vary)
(config)# ethersat loopback testsideport port ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
(config)# ethersat loopback testsideport port GigabitEthernet ?
    <port_type_list>    Port list in 1/1-24
(config)# ethersat loopback testsideport port GigabitEthernet 1/2 ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
    <cr>
(config)#
```

Example 4: Configure the EtherSAT **peerproto** parameters:

```
(config)# ethersat peerproto ?
    disable    disable  peerproto
    enable     enable peerproto
(config)# ethersat peerproto enable
Can't set ethersat flags
(config)# ethersat peerproto disable
Can't set ethersat flags
(config)#
```

Example 56: Create a new EtherSAT **profile**:

```
(config)# ethersat profile ?
    <1-16>    profile number from 1-16
    new       Create a new ethersat profile
(config)# ethersat profile new ?
    <1-16>    profile number from 1-16
(config)# ethersat profile new 2 ?
    name    Option to name the profile.
    <cr>
(config)# ethersat profile new 2 name ?
    <word32>    The profile name, max of 256 characters.
(config)# ethersat profile new 2 name ESatPrf2 ?
    <cr>
(config)# ethersat profile new 2 name ESatPrf2
Profile number 2 and name "ESatPrf2"
(config)# eth ?
    collector    EtherSAT Collector [enable|disable]
    loopback     TN ethersat loopback
    peerproto    EtherSAT PeerProto
    profile      ethersat profile
    test
    <cr>
(config)# eth profile ?
    <1-16>    profile number from 1-16
    new       Create a new ethersat profile
```

```
(config)# eth profile 2 ?
    clearpcp         Clear all yellow frame PCP values.
    dm-threshold     DM threshold <1-5000000> in usec.
    dmv-threshold    DMV threshold <1-5000000> in usec.
    flratio          Frame loss ratio.
    framefill        Set the Frame Filling mode (default is PRBS).
    frmencaps        Configure the Frame Encapsulation Type.
    linerate         Configure CBS Line Rate.
    name             Option to name the profile.
    ratedecstep      Configure Rate Decrease Step
    sizemix          Configure Frame Size Mix
    steplength       Configure the step length.
    testmode         Set the profile testmode.
    teststep         Set the profile test steps
    yellowpcp        Configure Yellow Frames PCP Values.
    yellowpcpmask    Configure Yellow Frames PCP Values in hex.
    <cr>
(config)# eth profile 2
```

Example 5: Configure an existing (created) EtherSAT **profile**:

```
(config)# ethersat profile 1 ?
    clearpcp         Clear all yellow frame PCP values.
    dm-threshold     DM threshold <1-5000000> in usec.
    dmv-threshold    DMV threshold <1-5000000> in usec.
    flratio          Frame loss ratio.
    framefill        Set the Frame Filling mode (default is PRBS).
    frmencaps        Configure the Frame Encapsulation Type.
    linerate         Configure CBS Line Rate.
    name             Option to name the profile.
    ratedecstep      Configure Rate Decrease Step
    sizemix          Configure Frame Size Mix
    steplength       Configure the step length.
    testmode         Set the profile testmode.
    teststep         Set the profile test steps
    yellowpcp        Configure Yellow Frames PCP Values.
    yellowpcpmask    Configure Yellow Frames PCP Values in hex.
    <cr>
(config)# eth pro 1 clear ?
    dm-threshold     DM threshold <1-5000000> in usec.
    dmv-threshold    DMV threshold <1-5000000> in usec.
    flratio          Frame loss ratio.
    framefill        Set the Frame Filling mode (default is PRBS).
    frmencaps        Configure the Frame Encapsulation Type.
    linerate         Configure CBS Line Rate.
    name             Option to name the profile.
    ratedecstep      Configure Rate Decrease Step
    sizemix          Configure Frame Size Mix
    steplength       Configure the step length.
    testmode         Set the profile testmode.
    teststep         Set the profile test steps
    yellowpcp        Configure Yellow Frames PCP Values.
    yellowpcpmask    Configure Yellow Frames PCP Values in hex.
    <cr>
(config)# eth pro 1 clear dm-threshold ?
```

```
    <1-5000000>    Delay Measurement Threshold accepts 8 values, low to high,
                   last value is always 5000000us.Minimum value is 30us.
(config)# eth pro 1 clear dm-threshold 50000 ?
    dmv-threshold    DMV threshold <1-5000000> in usec.
    flratio          Frame loss ratio.
    framefill        Set the Frame Filling mode (default is PRBS).
    frmencaps        Configure the Frame Encapsulation Type.
    linerate         Configure CBS Line Rate.
    name             Option to name the profile.
    ratedecstep      Configure Rate Decrease Step
    sizemix          Configure Frame Size Mix
    steplength       Configure the step length.
    testmode         Set the profile testmode.
    teststep         Set the profile test steps
    yellowpcp        Configure Yellow Frames PCP Values.
    yellowpcpmask    Configure Yellow Frames PCP Values in hex.
    <cr>
(config)# eth pro 1 clear dm-threshold 50000 dmv-threshold ?
    <1-5000000>    Delay Measurement Variation Threshold accepts 8 values, low
                   to high, last value is always 5000000us. Minimum value is
                   30us.
(config)# eth pro 1 clear dm-threshold 50000 dmv-threshold 100000 ?
    flratio          Frame loss ratio.
    framefill        Set the Frame Filling mode (default is PRBS).
    frmencaps        Configure the Frame Encapsulation Type.
    linerate         Configure CBS Line Rate.
    name             Option to name the profile.
    ratedecstep      Configure Rate Decrease Step
    sizemix          Configure Frame Size Mix
    steplength       Configure the step length.
    testmode         Set the profile testmode.
    teststep         Set the profile test steps
    yellowpcp        Configure Yellow Frames PCP Values.
    yellowpcpmask    Configure Yellow Frames PCP Values in hex.
    <cr>
(config)# $ pro 1 clear dm-threshold 50000 dmv-threshold 100000 flratio ?
    <uint>    The FLR percentage: min of 4 digits (1000 = 10.00).
(config)# $ pro 1 clear dm-threshold 50000 dmv-threshold 100000 flratio 1000 ?
    framefill        Set the Frame Filling mode (default is PRBS).
    frmencaps        Configure the Frame Encapsulation Type.
    linerate         Configure CBS Line Rate.
    name             Option to name the profile.
    ratedecstep      Configure Rate Decrease Step
    sizemix          Configure Frame Size Mix
    steplength       Configure the step length.
    testmode         Set the profile testmode.
    teststep         Set the profile test steps
    yellowpcp        Configure Yellow Frames PCP Values.
    yellowpcpmask    Configure Yellow Frames PCP Values in hex.
    <cr>
(config)# $-threshold 50000 dmv-threshold 100000 flratio 1000 framefill ?
    fixed    Fixed pattern of 4 octets.
    prbs     PRBS (pseudo-random bit stream).
```

```
(config)# $-threshold 50000 dmv-threshold 100000 flratio 1000 framefill prbs ?
    frmencaps        Configure the Frame Encapsulation Type.
    linerate         Configure CBS Line Rate.
    name             Option to name the profile.
    ratedecstep      Configure Rate Decrease Step
    sizemix          Configure Frame Size Mix
    steplength       Configure the step length.
    testmode         Set the profile testmode.
    teststep         Set the profile test steps
    yellowpcp        Configure Yellow Frames PCP Values.
    yellowpcpmask    Configure Yellow Frames PCP Values in hex.
    <cr>
(config)# $0 dmv-threshold 100000 flratio 1000 framefill prbs frmencaps ?
    L2      L2 frame format layer.
    L3      L3 frame format layer with configurable IP header.
    <cr>
(config)# $0 dmv-threshold 100000 flratio 1000 framefill prbs frmencaps L2 ?
    ceth-test    L2 Custom Ethernet test.
    eth-test     L2 EthTest.
    llc-snap     L2 LLC/SNAP test.
    <cr>
(config)# $old 100000 flratio 1000 framefill prbs frmencaps L2 eth-test ?
    meglevel    EthTst SOAM MEG level.
    <cr>
(config)# $0 flratio 1000 framefill prbs frmencaps L2 eth-test meglevel ?
    <0-7>    MEG level value <0-7>.
(config)# $0 flratio 1000 framefill prbs frmencaps L2 eth-test meglevel 4 ?
    <cr>
(config)# $0 flratio 1000 framefill prbs frmencaps L2 eth-test meglevel 4
(config)#
```

Example 7: Create a new EtherSAT **test**:

```
(config)# ethersat test ?
    new
    results    EtherSAT Test Results
    testid     EtherSAT Test Number
(config)# ethersat test new ?
    <1-16>    Test Number <1-16>
(config)# ethersat test new 1 ?
    profile     Ethersat profile number
    testname    Ethersat test name
(config)# ethersat test new 1 profile ?
    <1-16>    Profile number <1-16>
(config)# ethersat test new 1 profile 1 ?
    cip    Ethersat collector address
(config)# ethersat test new 1 profile 1 cip ?
    <ipv4_addr>    Collector IP address A.B.C.D
(config)# ethersat test new 1 profile 1 cip 192.168.1.30 ?
    cinport    Collector ingress port
(config)# ethersat test new 1 profile 1 cip 192.168.1.30 cinport ?
    <1-28>    Collector Port <1-28>
(config)# ethersat test new 1 profile 1 cip 192.168.1.30 cinport 2 ?
    inport    Initiator Ingress port
(config)# ethersat test new 1 profile 1 cip 192.168.1.30 cinport 2 inport ?
    <1-28>    Initiator Port <1-28>
(config)# ethersat test new 1 profile 1 cip 192.168.1.30 cinport 2 inport 3 ?
```

```
    inencaps-type    Ingress tag type options
(config)# $ profile 1 cip 192.168.1.30 cinport 2 inport 3 inencaps-type ?
    c-tag     Subscriber VLAN tag
    cc-tag    Double tagged: Two C-tags
    cs-tag    Double tagged: One C-tag, one S-tag
    none      No ingress tagging used on this test
    s-tag     Service VLAN tag
(config)# $ cip 192.168.1.30 cinport 2 inport 3 inencaps-type c-tag ?
    egencaps-type    Egress tag type options
    ipcp             Ingress inner PCP value
    ivid             Ingress inner VLAN ID
    opcp             Ingress outer PCP value
    ovid             Ingress outer VLAN ID
(config)# $68.1.30 cinport 2 inport 3 inencaps-type c-tag egencaps-type ?
    c-tag     Subscriber VLAN tag
    cc-tag    Double tagged: Two C-tags
    cs-tag    Double tagged: One C-tag, one S-tag
    none      No Egress tagging used on this test
    s-tag     Service VLAN tag
(config)# $nport 2 inport 3 inencaps-type c-tag egencaps-type s-tag ?
    ipcp    Egress inner PCP value
    ivid    Egress inner VLAN ID
    opcp    Egress outer PCP value
    ovid    Egress outer VLAN ID
    <cr>
(config)# $nport 2 inport 3 inencaps-type c-tag egencaps-type s-tag ipcp ?
    <0-7>    <0-7>
(config)# $nport 2 inport 3 inencaps-type c-tag egencaps-type s-tag ipcp 2 ?
    ivid    Egress inner VLAN ID
    opcp    Egress outer PCP value
    ovid    Egress outer VLAN ID
    <cr>
(config)# $port 3 inencaps-type c-tag egencaps-type s-tag ipcp 2 ivid ?
    <0-4095>    vlan ID <0-4095>
(config)# $port 3 inencaps-type c-tag egencaps-type s-tag ipcp 2 ivid 2 ?
    opcp    Egress outer PCP value
    ovid    Egress outer VLAN ID
    <cr>
(config)# $port 3 inencaps-type c-tag egencaps-type s-tag ipcp 2 ivid 2 opcp ?
    <0-7>    <0-7>
(config)# $ncaps-type c-tag egencaps-type s-tag ipcp 2 ivid 2 opcp 2 ?
    ovid    Egress outer VLAN ID
    <cr>
(config)# $ncaps-type c-tag egencaps-type s-tag ipcp 2 ivid 2 opcp 2 ovid ?
    <vlan_id>    vlan ID <0-4095>
(config)# $ncaps-type c-tag egencaps-type s-tag ipcp 2 ivid 2 opcp 2 ovid 20 ?
    <cr>
(config)# $ncaps-type c-tag egencaps-type s-tag ipcp 2 ivid 2 opcp 2 ovid 20
E ether_sat 00:52:41 14/saDbTestFindEgressPort#2376: Error: SA: Can't find ECE for VID 0, port 3
Version      : S4224 (standalone) 2.2.0
Build Date   : 2015-05-28T22:12:33-05:00
Warning: Return addresses are highly unreliable (code seems to be compiled with -O2)
```

Parameters: **ethersat test new** <testid> { [testname <testname>] } { profile <pid> } { cip <caddr> } { cinport <cinp> } { inport <inp> } { inencaps-type { none | c-tag | s-tag | cs-tag | cc-tag } [ivid <itvid>] [ipcp <inpcp>] [ovid <otvid>] [opcp <outpcp>] } { egencaps-type { none | c-tag | s-tag | cs-tag | cc-tag } [ivid <egitvid>] [ipcp <eginpcp>] [ovid <egotvid>] [opcp <egoutpcp>] }

Example 7: Configure an existing (already created and saved) EtherSAT **test**:

```
(config)# ethersat test ?
    new
    results    EtherSAT Test Results
    testid     EtherSAT Test Number
(config)# ethersat test results ?
    testid    Ethersat Test Number
(config)# ethersat test results testid ?
    <1-16>    Test number
(config)# ethersat test results testid 2 ?
    all           All test results
    b2b           B2B (Back-to-back) report
    export        Export: Save a report to a file on a TFTP server
    flr           FLR (Frame Loss Ratio) report
    latency       Latency report
    throughput    Throughput report
(config)# ethersat test results testid 2 all ?
    <cr>
(config)# ethersat test results testid 2 all
Error: unable to get test with Id 2
(config)# ethersat test ?
    new
    results    EtherSAT Test Results
    testid     EtherSAT Test Number
(config)# ethersat test testid ?
    <1-16>    <1-16>
(config)# ethersat test testid 2 ?
    bandwidth      Bandwidth parameters from a configured policer
    cbs            Configure CBS (Committed Burst Size)
    cip            Ethersat collector address
    cir            Configure CIR (Committed Information Rate)
    delete         Delete an EtherSAT test number
    ebs            Configure EBS (Excess Burst Size)
    egress         EtherSAT Test Egress Encapsulation
    eir            Configure EIR (Excess Information Rate)
    ingress        EtherSAT Test Ingress Encapsulation
    profile        Ethersat profile number
    showconfig     Display a specific EtherSAT Test configuration
    start          Start an Ethersat test
    stop           Stop an Ethersat test
    testmacaddr    EtherSAT Test MAC address
    testname       Ethersat Test Name
    <cr>
(config)# ethersat test testid 2
```

Parameters:

ethersat test results { testid <tid> } [all | throughput | latency | flr | b2b] { export <reportname> <tftpurl> }
ethersat test { testid <tid> } [testname <testname>] [delete] [start] [stop] [profile <pid>] [cip <caddr>] [bandwidth { policer-id <polid> }] [cir <cir>] [cbs <cbs>] [eir <eir>] [ebs <ebs>] [testmacaddr <macaddr>] [showconfig] [ingress [inencaps-type { none | c-tag | s-tag | cs-tag | cc-tag}] [ivid <itvid>] [ipcp <inpcp>] [ovid <otvid>] [opcp <outpcp>]] [egress [egencaps-type { none | c-tag | s-tag | cs-tag | cc-tag }] [ivid <egitvid>] [ipcp <eginpcp>] [ovid <egotvid>] [opcp <egoutpcp>]](config)# ethersat test testid

EtherSAT Messages

Message:

ethersat loopback state set failed. Check that the shared port is internal and try again
etherset loopback testsideport set failed. Check that the shared port is internal and try again
etherset loopback timeout set failed. Check that the shared port is internal and try again
etherset loopback smac set failed. Check that the shared port is internal and try again
etherset loopback vid set failed. Check that the shared port is internal and try again

Meaning: The EtherSAT loopback test failed because the shared port is not set to internal mode.
Recovery: Set the shared port to internal mode using the (config)# command `sharedport internal` and try the loopback test again.

Problem: The S4224 or S4140 cannot be used as an Ethersat loopback device.
Workaround: Use an S3280 or other NID as the loopback device.

Problem: The 10GE SFP+ ports cannot be set as Test Side Ports. They can be entered and the state set to active but refreshing the page changes them to port 1.
Workaround: Use the 100/1000 SFP ports as Test Side Ports.

Message: *Error: tn_ether_sat_lb_conf_set failed*

Meaning: The Factory Defaults web command does not reset Service Actation Loopback. After the Factory Defaults web command successfully completes, the Service Activation Loopback is still active. However, the shared port has been reset to external and at this point the loopback can not be set to inactive. When attempted, the following error is reported on the CLI:

E web 01:42:26 76/handler_config_tn_ether_sat#126: Error: tn_ether_sat_lb_conf_set failed

Recovery: To deactivate the loopback, set the shared port back to internal.

Command: Configure EVC

Syntax: config# **evc** (see parameters descriptions below)
Description: Configure EVC in terms of EVC ID, ECE, name, and Policer. These commands configure Ethernet Virtual Connections (EVCs)and their configurations using the ECEs. The MEF standards describe services provided to customers at User Network Interfaces (UNIs). Inside provider networks, nodes are connected using Internal Network-to- Network Interfaces (I-NNIs). Connections between service providers are done using External Network-to-Network Interfaces (E-NNIs). An Ethernet Virtual Connection (EVC) is an association of two or more UNIs. Three EVC types are defined:

- E-Line: Point-to-point connection of two UNIs.
- E-LAN: Multipoint-to-multipoint connection of two or more UNIs.
- E-Tree: Rooted-multipoint connection between leaf and root UNIs. Frames are not forwarded between leaf UNIs.

The MEF defines a number of attributes associated with a UNIs and EVCs. These attributes include mappings of customer VLAN IDs to EVCs, ingress bandwidth profiles, processing of L2 control protocols (L2CP), etc.

The S4224 EVC (Ethernet Virtual Connection) commands let you configure S4224 Ethernet services in terms of EVCs and ECEs (EVC Control Entries). Only Provider Bridge based EVCs are supported on the S4224. 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.

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.

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.

Note: You must set up an EVC before trying to set up a related ECE.
Mode: (config)#
Example 1: Show the various EVC configurable parameters.

```
(config)# evc?
    evc    Ethernet Virtual Connections
(config)# evc ?
    <1-4096>    EVC identifier
    ece         EVC Control Entry
    name        Set name of EVC
    policer     Policer (ingress bandwith profile)
    update      Update existing entry
(config)#
```

Example 2: Show EVC 1 configurable parameters.

```
(config)# evc 1 ?
    interface    Setup NNI
    ivid         Setup internal EVC VLAN ID
    learning     Setup learning
    policer      Policer (ingress bandwith profile)
    vid          Setup EVC VLAN ID
    <cr>
(config)# evc 1
```

Example 3: Setup EVC NNI (interface):

```
(config)# evc 2 interface ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
(config)# evc 2 interface 10GigabitEthernet ?
    <port_type_list>    Port list in 1/1-4
(config)# evc 2 interface 10GigabitEthernet 1/2-4 ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
    ivid                Setup internal EVC VLAN ID
    learning            Setup learning
    policer             Policer (ingress bandwith profile)
    <cr>
(config)# evc 2 interface 10GigabitEthernet 1/2-4 ivid ?
    <vlan_id>    Internal VLAN ID
(config)# evc 2 interface 10GigabitEthernet 1/2-4 ivid 10 ?
    learning    Setup learning
    policer     Policer (ingress bandwith profile)
    <cr>
(config)# evc 2 interface 10GigabitEthernet 1/2-4 ivid 10 learning ?
    disable    Disable learning
    policer    Policer (ingress bandwith profile)
    <cr>
(config)# evc 2 interface 10GigabitEthernet 1/2-4 ivid 10 learning pol ?
    <1-2048>    Policer ID
    discard     Map to policer discarding all frames
    none        Map to policer allowing all frames
(config)#
```

EVC Command Parameters

```
(config)# evc??
evc [ update ] <evc_id> { [ vid <evc_vid> ] } [ ivid <ivid> ] [ interface ( <port_type> [ <port_list> ] )
] [ learning [ disable ] ] [ policer { <policer_id> | none | discard } ] [ inner-tag add { [ type { none |
c-tag | s-tag | s-custom-tag } ] [ vid-mode { normal | tunnel } ] [ vid <it_add_vid> ] [ preserve [
disable ] ] [ pcp <it_add_pcp> ] [ dei <it_add_dei> ] }*1 ] [ outer-tag add vid <ot_add_vid> ] [ pw [
<pw_num_list> ] [ split-horizon <pw_num_list_split_horizon> ] ] evc ece [ update ] <ece_id> [ next {
<ece_id_next> | last } ] [ lookup { basic | advanced } ] [ interface ( <port_type> [ <port_list> ] ) ] [
smac { <smac> | any } ] [ dmac { <dmac> | unicast | multicast | broadcast | any } ] [ outer-tag {
[ match { [ type { untagged | tagged | c-tagged | s-tagged | any } ] [ vid { <ot_match_vid> | any } ] [
pcp { <ot_match_pcp> | any } ] [ dei { <ot_match_dei> | any } ] }*1 ] [ add { [ mode { enable | disable }
] [ vid <ot_add_vid> ] [ preserve [ disable ] ] [ pcp-mode { classified | fixed | mapped } ] [ pcp
<ot_add_pcp> ] [ dei-mode { classified | fixed | dp } ] [ dei <ot_add_dei> ] }*1 ] }*1 ] [
inner-tag { [ match { [ type { untagged | tagged | c-tagged | s-tagged | any } ] [ vid { <it_match_vid> |
any } ] [ pcp { <it_match_pcp> | any } ] [ dei { <it_match_dei> | any } ] }*1 ] [ add { [ type { none | c-
tag | s-tag | s-custom-tag } ] [ vid <it_add_vid> ] [ preserve [ disable ] ] [ pcp-mode { classified |
fixed | mapped } ] [ pcp <it_add_pcp> ] [ dei-mode { classified | fixed | dp } ] [ dei <it_add_dei> ] }*1
] }*1 ] [ frame-type { any | { ipv4 [ proto { <pr4> | udp | tcp | any } ] [ dscp { <dscp4> | any } ] [ sip
{ <sip4> | any } ] [ dip { <dip4> | any } ] [ fragment { yes | no | any } ] [ sport { <sp4> | any } ] [
dport {<dp4> | any } ] } | { ipv6 [ proto { <pr6> | udp | tcp | any } ] [ dscp { <dscp6> | any } ] [ sip {
<sip6> | any } ] [ dip { <dip6> | any } ] [ sport { <sp6> | any } ] [ dport { <dp6> | any } ] } | { etype
[ etype-value { <etype_value> | any } ] [ etype-data { <etype_data> | any } [ <etype_mask> ] ] } | { llc [
dsap {<dsap> | any } ] [ ssap { <ssap> | any } ] [ control { <control> | any } ] [ llc-data { <llc_data> |
any } [ <llc_mask> ] ] } | { snap [ oui { <oui> | any } ] [ pid { <pid> | any } ] } | { l2cp { stp | pause
| lacp | lamp | loam | dot1x | elmi | pb | pb-gvrp | lldp | gmrp | gvrp | uld | pagp | pvst | cisco-vlan |
cdp | vtp | dtp | cisco-stp | cisco-cfm } } } ] [ direction { both | uni-to-nni | nni-to-uni } ] [ rule-
type { both | rx | tx } ] [ tx-lookup { vid | pcp-vid | isdx} ] [ l2cp { [ mode { tunnel | peer | forward
| discard } ] [ tmac { cisco | custom } ] }*1 ] [ evc { <evc_id> | none } ] [ policer { <policer_id> |
none | discard | evc } ] [ pop <pop> ] [ policy <policy_no> ] [ cos { <cos> | disable } ] [ dpl { <dpl> |
disable } ] evc name <evc_id> <evc_name> evc policer [ update ] <policer_id> [ { enable | disable } ] [
type { mef | single } ] [ mode { coupled | aware | blind } ] [ rate-type { line | data } ] [ cir <cir> ] [
cbs <cbs> ] [ eir <eir> ] [ ebs <ebs> ]
```

Command: Configure EVC ECE

Syntax: **evc ece** : ECE idenfifier <EceId : 1-4096>
evc ece update : Update existing entry <EceId : 1-4096>.

Description: Configure a new or existing EVC Control Entry. **Note**: You must set up an EVC before trying to set up a related ECE.

direction Setup ECE direction.
dmac Setup matched Destination MAC.
evc EVC mapping.
frame-type Setup matched frame type.
inner-tag Setup inner tag options.
interface Setup UNI.
next Setup the ECE ID of the next entry.
outer-tag Setup outer tag options.
policer Policer (ingress bandwith profile).
policy Setup ACL policy.
pop Setup tag popping.
<cr>

Mode: (config)

Example: *1* Display the various EVC ECE configurable parameters.

```
 (config)# evc ece 1 ?
    direction     Setup ECE direction
    dmac          Setup matched DMAC
    evc           EVC mapping
    frame-type    Setup matched frame type
    inner-tag     Setup inner tag options
    interface     Setup UNI
    next          Setup the ECE ID of the next entry
    outer-tag     Setup outer tag options
    policer       Policer (ingress bandwith profile)
    policy        Setup ACL policy
    pop           Setup tag popping
    <cr>
(config)# evc ece 1 direction ?
    both          Bidirectional traffic flow
    nni-to-uni    NNI-to-UNI traffic flow
    uni-to-nni    UNI-to-NNI traffic flow
(config)# evc ece 1 dmac ?
    <mac_addr>    Matched DMAC
    any           Match any DMAC
    broadcast     Match broadcast DMAC
    multicast     Match multicast DMAC
    unicast       Match unicast DMAC
(config)# evc ece 1 evc ?
    <1-4096>    EVC identifier
    none        Map to no EVC ID
(config)# evc ece 1 frame-type ?
    any          Match any frame type
    direction    Setup ECE direction
    dmac         Setup matched DMAC
    evc          EVC mapping
    inner-tag    Setup inner tag options
    interface    Setup UNI
    ipv4         Match IPv4 frames
```

```
    ipv6         Match IPv6 frames
    next         Setup the ECE ID of the next entry
    outer-tag    Setup outer tag options
    policer      Policer (ingress bandwith profile)
    policy       Setup ACL policy
    pop          Setup tag popping
    <cr>
(config)# evc ece 1 inner-tag ?
    add      Setup inner tag add properties
    match    Setup inner tag match properties
(config)# evc ece 1 interface ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
(config)# evc ece 1 next ?
    <1-4096>    Select ECE ID of an existing entry
    last        Make the ECE the last entry
(config)# evc ece 1 outer-tag ?
    add      Setup outer tag add properties
    match    Setup outer tag match properties
(config)# evc ece 1 policer ?
    <1-2048>    Policer ID
    discard     Map to policer discarding all frames
    evc         Use policer setup for EVC
    none        Map to policer allowing all frames
(config)# evc ece 1 policy ?
    <0-255>    ACL policy
(config)# evc ece 1 pop ?
    <0-2>    Number of tags popped
(config)# evc ece 1 pop
(config)#
```

Note: If an EVC Up MEP is created you should enable 'Tunnel' for L2CP Mode in the EVC ECE if using Spanning Tree/LLDP per MEF 6.1. The MEP will receive a loss of CCM if tunnel mode is not enabled. Note that Tunnel mode is not available at the Port level because it is an EVC Service attribute. The loss of CCM generally occurs because of the difference between CCM intervals, STP restoration times and/or LLDP re-initialization.

Example 4: Display all of the EVC ECE parameters:

```
(config)# evc ece?
    ece    EVC Control Entry
(config)# evc ece 1 evc 1?
evc ece [ update ] <ece_id> [ next { <ece_id_next> | last } ] [ lookup { basic | advanced } ] [ interface
( <port_type> [ <port_list> ] ) ] [ smac { <smac> | any } ] [ dmac { <dmac> | unicast | multicast |
broadcast | any } ] [ outer-tag {[ match { [ type { untagged | tagged | c-tagged | s-tagged | any } ] [
vid { <ot_match_vid> | any } ] [ pcp { <ot_match_pcp> | any } ] [ dei { <ot_match_dei> | any } ] }*1 ] [
add { [ mode { enable | disable } ] [ vid <ot_add_vid> ] [ preserve [ disable ] ] [ pcp-mode { classified
| fixed | mapped } ] [ pcp <ot_add_pcp> ] [ dei-mode { classified | fixed | dp } ] [ dei <ot_add_dei> ]
}*1 ] }*1 ] [inner-tag { [ match { [ type { untagged | tagged | c-tagged | s-tagged | any } ] [ vid {
<it_match_vid> | any } ] [ pcp { <it_match_pcp> | any } ] [ dei { <it_match_dei> | any } ] }*1 ] [ add { [
type { none | c-tag | s-tag | s-custom-tag } ] [ vid <it_add_vid> ] [ preserve [ disable ] ] [ pcp-mode {
classified | fixed | mapped } ] [ pcp <it_add_pcp> ] [ dei-mode { classified | fixed | dp } ] [ dei
<it_add_dei> ] }*1 ] }*1 ] [ frame-type { any | { ipv4 [ proto { <pr4> | udp | tcp | any } ] [ dscp {
<dscp4> | any } ] [ sip { <sip4> | any } ] [ dip { <dip4> | any } ] [ fragment { yes | no | any } ] [
sport { <sp4> | any } ] [ dport {<dp4> | any } ] } | { ipv6 [ proto { <pr6> | udp | tcp | any } ] [ dscp {
<dscp6> | any } ] [ sip { <sip6> | any } ] [ dip { <dip6> | any } ] [ sport { <sp6> |any } ] [ dport {
<dp6> | any } ] } | { etype [ etype-value { <etype_value> | any } ] [ etype-data { <etype_data> | any } [
<etype_mask> ] ] } | { llc [ dsap {<dsap> | any } ] [ ssap { <ssap> | any } ] [ control { <control> | any
} ] [ llc-data { <llc_data> | any } [ <llc_mask> ] ] } | { snap [ oui { <oui> | any } ] [ pid { <pid> |
any } ] } | { l2cp { stp | pause | lacp | lamp | loam | dot1x | elmi | pb | pb-gvrp | lldp | gmrp | gvrp |
uld | pagp | pvst | cisco-vlan | cdp | vtp | dtp | cisco-stp | cisco-cfm } } } ] [ direction { both | uni-
to-nni | nni-to-uni } ] [ rule-type { both | rx | tx } ] [ tx-lookup { vid | pcp-vid | isdx} ] [ l2cp { [
mode { tunnel | peer | forward | discard } ] [ tmac { cisco | custom } ] }*1 ] [ evc { <evc_id> | none } ]
[ policer { <policer_id> | none | discard | evc } ] [ pop <pop> ] [ policy <policy_no> ] [ cos { <cos> |
disable } ] [ dpl { <dpl> | disable } ]
(config)# evc ece 1 evc 1
```

Messages

```
(config)# evc ece 1 int Gi 1/2 outer-tag match type tagged vid 10-11
% ECE 1: GigabitEthernet 1/2 is an NNI
(config)# evc ece 1 int Gi 1/3 outer-tag match type tagged vid 10-11
(config)# evc ece 2 int Gi 1/3 outer-tag match type tagged vid 10-11
(config)#
(config)# evc ece 2 int Gi 1/3 outer-tag match type tagged vid 10-12
                                                               ^
% Invalid word detected at '^' marker.

(config)# evc ece 2 int Gi 1/3 outer-tag match type tagged vid 11-12
                                                               ^
% Invalid word detected at '^' marker.

(config)# evc ece 2 int Gi 1/3 outer-tag match type tagged vid 10-11
(config)#
```

Meaning: *The range needs to be based on a bit mask. For example:\n160 (10100000 in binary) can go to\n161 (10100001)\n163 (10100011)\n167 (10100111)\n175 (10101111) or\n191 (10111111).*

Recovery: Change the VID range to a range such as 10-11.

Command: Configure EVC Policer

Syntax: **evc policer** [update] <policer_id> [{ enable | disable }] [type { mef | single }] [mode { coupled | aware | blind }] [rate-type { line | data }] [cir<cir>] [cbs <cbs>] [eir <eir>] [ebs <ebs>]

Description: Configure an new or update an existing EVC Policer (ingress bandwith profile).
This is technically not a leaky bucket but it is referred to as a token bucket profile in MEF10.2 (which does not mention a leaky bucket). This profile is only used for the EVC configuration. The bucket is essentially not "leaking"; the frames may be marked as yellow so they do not actually leave the bucket profile. It also is important to distinguish between the two types of traffic conditioning. The type in the QoS section is a port based single-rate conditioner and the MEF policer is a two-rate three color marker conditioner (trTCM). The parameters are:

<**1**-**2048**> : Policer ID

update : Update an existing entry <1-**2048**>.

Mode: (config)#

Example 1:

```
(config)# evc policer 1 ?
    cbs          Setup CBS
    cir          Setup CIR
    disable      Disable policer
    ebs          Setup EBS for MEF policer
    eir          Setup EIR for MEF policer
    enable       Enable policer
    mode         Setup policer mode
    rate-type    Setup rate type
    type         Setup policer type
    <cr>
(config)# evc policer 1
```

Example 2:

```
(config)# evc policer 1 rate-type ?
    data    Data rate policing
    line    Line rate policing
(config)# evc policer 1 rate-type  data ?
    cbs        Setup CBS
    cir        Setup CIR
    disable    Disable policer
    ebs        Setup EBS for MEF policer
    eir        Setup EIR for MEF policer
    enable     Enable policer
    mode       Setup policer mode
    type       Setup policer type
    <cr>
(config)# evc policer 1 rate-type line ?
    cbs        Setup CBS
    cir        Setup CIR
    disable    Disable policer
    ebs        Setup EBS for MEF policer
    eir        Setup EIR for MEF policer
    enable     Enable policer
    mode       Setup policer mode
    type       Setup policer type
    <cr>
(config)# evc policer 1 rate-type line
```

Example 3:

```
(config)# evc policer 1 cbs ?
    <Cbs : 0-100000>    Committed Burst Size [bytes]
```

Example 4:
```
(config)# evc policer 1 cir ?
    <Cir : 0-10000000>    Committed Information Rate [kbps]
(config)# evc policer 1 disable ?
    cbs           Setup CBS
    cir           Setup CIR
    ebs           Setup EBS for MEF policer
    eir           Setup EIR for MEF policer
    mode          Setup policer mode
    rate-type     Setup rate type
    type          Setup policer type
    <cr>
```

Example 5:
```
(config)# evc policer 1 ebs ?
    <Ebs : 0-100000>    Excess Burst Size [bytes]
```

Example 6:
```
(config)# evc policer 1 eir ?
    <Eir : 0-10000000>    Excess Information Rate [kbps]
```

Example 7:
```
(config)# evc policer 1 enable ?
    cbs           Setup CBS
    cir           Setup CIR
    ebs           Setup EBS for MEF policer
    eir           Setup EIR for MEF policer
    mode          Setup policer mode
    rate-type     Setup rate type
    type          Setup policer type
    <cr>
```

Example 8:
```
(config)# evc policer 1 mode ?
    aware      Color-aware mode
    coupled    Coupling mode
```

Example 9:
```
(config)# evc policer 1 type ?
    mef       MEF ingress bandwidth profile
    single    Single bucket policer
(config)# evc policer 1 mode aware ?
    cbs           Setup CBS
    cir           Setup CIR
    disable       Disable policer
    ebs           Setup EBS for MEF policer
    eir           Setup EIR for MEF policer
    enable        Enable policer
    rate-type     Setup rate type
    type          Setup policer type
    <cr>
(config)# evc policer 1 mode coupled ?
    cbs           Setup CBS
    cir           Setup CIR
    disable       Disable policer
    ebs           Setup EBS for MEF policer
    eir           Setup EIR for MEF policer
    enable        Enable policer
    rate-type     Setup rate type
    type          Setup policer type
    <cr>
```

EVC Policer Parameters

EVC Policers can be created or modified with the parameters below. These policers may be used to limit the traffic received on UNI ports.

Parameter	Valid Range	Default
Policer ID	1 to 2048. Two policer IDs are reserved and cannot be changed.	None
Policer Mode	Coupled or Aware: **aware** = Color-aware mode with coupling disabled. **coupled** = Coupling mode with coupling enabled. **blind** = Color-blind mode	aware
Type	EVC Policer type (MEF or Single): **mef** = MEF ingress bandwidth profile **single** = Single bucket policer	mef
CIR	Committed Information Rate [kbps] of the bandwidth profile: 0 to 10000000 kbps	0
CBS	Committed Burst Size [bytes] of the bandwidth profile: 0 to 100000 bytes	0
EIR	Excess Information Rate [kbps] of the bandwidth profile; 0 to 10000000 kbps	0
EBS	Excess Burst Size [bytes] of the bandwidth profile: 0-100000 bytes	0
Rate-type	Data or Line: **data** = Specifies that this bandwidth profile operates on data rate. **line** = Specifies that this bandwidth profile operates on line rate.	data
Type (Data type)	MEF or Single: **mef** = MEF ingress bandwidth profile **single** = Single bucket policer	mef

Ethernet Services Application Example

E-Line services are typically used to replace TDM private lines and use two dedicated UNI ports. It is the most common type of Ethernet Service. The transport-oriented Ethernet Private Line service provides an interconnection between switching or routing equipment in a private data network. This is an ideal service for a Subscriber that needs to manage its own network infrastructure and the Service Provider is providing point-to-point services between two designated UNIs at an agreed upon UNI port speed. An Ethernet Virtual Private Line service can be used to map one or more CE-VLAN IDs to an EVC if multiple services are required.

An EVPL service is commonly used for connecting Subscriber hub and branch locations.

An example EPL Service may be configured on two S4224s with the GUI or CLI:

Remove existing VLANs and change switchport interface mode to hybrid, default port-type will be C-Port:

```
#conf t
(config)#no interface vlan 2-4094
(config)#interface GigabitEthernet 1/2-4 10GigabitEthernet 1/1-2
(config-if)#switchport mode hybrid
(config-if)#exit
```

Establish the S-Port interface on GigabitEthernet port 1/3:

```
(config)#interface GigabitEthernet 1/3
(config-if)#switchport hybrid port-type s-port
(config-if)#exit
```

Define EVC with VID 11, IVID 1001 and NNI port as GigabitEthernet port 1/3. Configure Ethernet Control Entry 1 for EVC 1 with the UNI port as GigabitEthernet Port 1/2:

```
(config)#evc 1 vid 11 ivid 1001 interface GigabitEthernet 1/3
(config)#evc ece 1 interface GigabitEthernet 1/2 evc 1
```

Subscribers with multiple sites that need to be on the same LAN would configure an E-LAN Service. In an Ethernet Private LAN Service CE-VLAN ID and Class of Service preservation applies so typically no coordination with a Service Provider is needed. One or more Bandwidth Profile flows can be based on a CoS identifier. An EP-LAN Service is configured for all-to-one bundling and therefore services are port based with all CE-VLAN IDs mapping to a single EVC. In an Ethernet Virtual Private LAN service, the multipoint-to-multipoint EVC service has service multiplexing capability to support more than one EVC.

An example EP-LAN Service may be configured on two S4224s with the GUI or CLI. This service features a single EVC with one UNI port on device 1 and two UNI ports on device 2 using VID 11.

Device 1:

```
#conf t
(config)#no int vlan 2-4094
(config)#int Gi 1/2-4 2.5Gi 1/1-2
(config-if)#switchport mode hybrid
(config-if)#exit
(config)#int 10GigabitEthernet 1/2
(config-if)#switchport hybrid port-type s-port
(config-if)#exit
(config)#evc 3 vid 11 ivid 1001 interface 10GigabitEthernet 1/2 learning
```

Configure the EVC Ethernet Control Entry 1 for UNI port GigabitEthernet 1/2. All tagged frames are matched in EVC 3:

```
(config)#evc ece 1 interface GigabitEthernet 1/2 outer-tag match type tagged evc 3
```

On device 2 remove the VLANs and identify the s-port as on device 1. Then configure EVC 3 for ports GigabitEthernet 1/2 and 1/3:

```
(config)#evc 3 vid 11 ivid 1001 interface 10GigabitEthernet 1/2 learning
(config)#evc ece 1 interface GigabitEthernet 1/2,3 outer-tag match type tagged evc 3
```

Note: MAC learning is enabled for EVCs with more than two ports so that source addresses are learned for frames matching the EVC.

An Ethernet Private Tree Service can give subscribers the opportunity to interconnect multiple sites to provide services other than those resembling a LAN. This type of service is known as a rooted multi-point service because the root is able to communicate with the leaves but the leaves are not able to communicate. CE-VLAN tag preservation and tunneling of L2CP frames are features of an EP-Tree service where each UNI associated by an EVC has one EVC. An Ethernet Virtual Private Tree service can be used to interconnect participating UNIs to a well-defined access, or root point. For example if a customer has an EVP-LAN Service providing data connectivity between four UNIs while using an EVP-Tree service to provide video broadcasts from a video hub location. In an EVP-Tree service, at least one CE-VLAN ID is mapped to each EVC.

An E-Access service type can be used to create a broad range of Ethernet access services. An Access EPL service can provide a high degree of transparency for frames, similar to an EPL service such that the frames header and payload upon ingress at the UNI is delivered unchanged to the ENNI with the addition of an S-VLAN tag. The S-VLAN tag is removed upon delivery to the UNI from the ENNI. A Service Provider can use an Access EPL service from an Access Provider to deliver port-based Ethernet services. At the SP ENNI a unique SVLAN ID per Access EPL maps to a single OVC, or Operator Virtual Connection End Point. The Service Provider and Access Provider coordinate the value of the S-VLAN ID at the ENNI. There is no need for coordination between the Subscriber and Service Provider because all Service Frames at the UNI are mapped to a single OVC End Point. Alternatively, an Access EVPL can support multiple service instances including a mix of Access and EVC services.

An example Access EVPL service with two OVCs is provisioned with two OVC End Points on device 1. OVC EP1 will pass single tag frames with CE-VLAN ID 1 and OVC EP2 will pass single tag frames with CE-VLAN ID 2 on UNI Port 2 ingress. Device 2 also has two OVC End Points. OVC EP3 is mapped on device 2 and double tagged frames with S-VLAN ID 11 and CE-VLAN ID 1 will be seen on egress ENNI port 10GigabitEthernet 1/2. OVC EP 4 is mapped to device 2 and will have double tagged frames with S-VLAN ID 2 and CE-VLAN ID 2 on the same egress ENNI.

Device 1:

```
#conf t
(config)#no int vlan 2-4094
(config)#int Gi 1/2-4 2.5Gi 1/1-2
(config-if)#switchport mode hybrid
(config-if)#exit
(config)#int 10GigabitEthernet 1/2
(config-if)#switchport hybrid port-type s-port
(config-if)#exit
(config)#evc 1 vid 11 ivid 1001 interface 10GigabitEthernet 1/2
(config)#evc 2 vid 22 ivid 1002 interface 10GigabitEthernet 1/2
```

Configure the EVC Ethernet Control Entry 1 for UNI port GigabitEthernet 1/2. Tagged frames are matched with vid 0-1 with PCP 5 in OVC 5:

```
(config)#evc ece 1 interface GigabitEthernet 1/2 outer-tag match type tagged vid 0-1
add pcp 5 evc 3
```

Configure the EVC Ethernet Control Entry 2 also for UNI port GigabitEthernet 1/2. Untagged frames are matched with PCP 5 in OVC 5:

```
(config)#evc ece 2 interface GigabitEthernet 1/2 outer-tag match type untagged add
pcp 5 evc 3
```

Configure the final EVC Ethernet Control Entry 3 also for UNI port GigabitEthernet 1/2. Untagged frames are matched with PCP 5 in OVC 6:

```
(config)#evc ece 3 interface GigabitEthernet 1/2 outer-tag match type tagged add pcp
1 evc 4
```

Device 2:

```
#conf t
(config)#no int vlan 2-4094
(config)#int Gi 1/2-4 2.5Gi 1/1-2
(config-if)#switchport mode hybrid
(config-if)#exit
(config)#int 1/2 10GigabitEthernet 1/2
(config-if)#switchport hybrid port-type s-port
(config-if)#switchport hybrid allowed vlan 11,22
```

Configure both ports GigabitEthernet 1/2 and 10GigabitEthernet 1/2 as s-ports. Allow both S-VLAN IDs 11 and 22 on these ports. In this configuration, OVC 5 is represented by OVC End Points 1 and 2 and OVC6 by OVC End Points 3 and 4. In this way two Operator Virtual Connection services can exist on each ENNI.

Command: Exit Config Mode

Syntax: **config exit**
Description: Exit from Configuration mode.
Mode: (config)#
Example:
```
(config)# exit
#
```

Command: Enable GVRP Feature

Syntax: **gvrp**
Description: Enable GVRP feature. GVRP (GARP VLAN Registration Protocol) allows network devices to share VLAN information and to use the information to modify existing VLANs or create new VLANs, automatically.
Mode: (config) #
Example:
```
(config)# gvrp
(config)#
```

Command: Configure GVRP Max VLANs

Syntax: **gvrp max-vlans**
Description: Set the number of simultaneous VLANs that GVRP can control (1-4095).
Mode: (config)#
Example:
```
(config)# gvrp max-vlans 100
(config)# gvrp max-vlans 1000
(config)#
```

Related Commands: **show vlan status gvrp**

Command: Configure GVRP Time

Syntax: **gvrp time** { [join-time <1-20>] [leave-time <60-300>] [leave-all-time <1000-5000>] }*1

Description: GVRP (GARP VLAN Registration Protocol) allows network devices to share VLAN information and to use the information to modify existing VLANs or create new VLANs, automatically. This makes it easier to manage VLANs that span more than one switch. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices. See the IEEE standards page at http://standards.ieee.org/findstds/standard/802.1D-2004.html.

Mode: (config)#

Example 1: Display GVRP functions available:

```
(config)# gvrp?
    gvrp    Enable GVRP feature
    <cr>
(config)# gvrp ?
    max-vlans    Number of simultaniously VLANs that GVRP can control
    time         Config GARP protocol timer parameters. IEEE 802.1D-2004, clause 12.11.
    <cr>
(config)# gvrp?
gvrp
gvrp max-vlans <maxvlans>
gvrp time { [ join-time <jointime> ] [ leave-time <leavetime> ] [ leave-all-time
<leavealltime> ] }*1
(config)# gvrp time ?
    join-time         Set GARP protocol parameter JoinTime.
    leave-all-time    Set GARP protocol parameter LeaveAllTime.
    leave-time        Set GARP protocol parameter LeaveTime.
(config)# gvrp time join-time ?
    <Jointime : 1-20>    join-time in units of centi seconds. Range is 1-20. Default is 20.
(config)# gvrp time leave-all-time ?
    <Leavealltime : 1000-5000>    leave-all-time in units of centi seconds
                                  Range is 1000-5000. Default is 1000.
(config)# gvrp time leave-time ?
    <Leavetime : 60-300>    leave-time in units of centi seconds. Range is 60-300. Default is
60.
(config)# gvrp time leave-time
```

Example 2: Configure GVRP functions:

```
(config)# gvrp time join-time 15 leave-all-time ?
    <Leavealltime : 1000-5000>    leave-all-time in units of centi seconds
                                  Range is 1000-5000. Default is 1000.
(config)# gvrp time join-time 15 leave-all-time 2000 ?
    leave-time    Set GARP protocol parameter LeaveTime. See IEEE 802.1D-2004, clause 12.11
    <cr>
(config)# gvrp time join-time 15 leave-all-time 2000 leave-time ?
    <Leavetime : 60-300>    leave-time in units of centi seconds. Range is 60-300. Default is
60.
(config)# gvrp time join-time 15 leave-all-time 2000 leave-time 120
(config)#
```

Related Commands: **show vlan status gvrp**

Command: Configure Help

Syntax: **?**

Description: Description of the interactive help system. Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options. Two styles of help are provided:

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

Mode: (config)#

Example: Display the available help topics:

```
(config)# ?
    aaa              Authentication, Authorization and Accounting
    access           Access management
    access-list      Access list
    aggregation      Aggregation mode
    banner           Define a login banner
    clock            Configure time-of-day clock
    ddmi             DDMI Information
    default          Set a command to its defaults
    do               To run exec commands in config mode
    dot1x            IEEE Standard for port-based Network Access Control
    enable           Modify enable password parameters
    end              Go back to EXEC mode
    eps              Ethernet Protection Switching.
    erps             Ethernet Ring Protection Switching
    ethersat         ethersat (Service Activation Test)
    evc              Ethernet Virtual Connections
    exit             Exit from current mode
    gvrp             Enable GVRP feature
    help             Description of the interactive help system
    hostname         Set system's network name
    interface        Select an interface to configure
    ip               Internet Protocol
    ipmc             IPv4/IPv6 multicast configuration
    ipv6             IPv6 configuration commands
    lacp             LACP settings
    line             Configure a terminal line
    lldp             LLDP configurations.
    logging          System logging message
    loop-protect     Loop protection configuration
    mac              MAC table entries/configuration
    mep              Maintenance Entity Point
    monitor          Monitoring different system events
    mvr              Multicast VLAN Registration configuration
    no               Negate a command or set its defaults
    ntp              Configure NTP
    perf-mon         Performance Monitor
    port-security    Enable/disable port security globally.
    privilege        Command privilege parameters
    ptp              Precision time Protocol (1588)
    qos              Quality of Service
    radius-server    Configure RADIUS
    rmon             Remote Monitoring
    sharedport       Shared Port status: Internal or External
    snmp-server      Set SNMP server's configurations
    spanning-tree    Spanning Tree protocol
    switchport       Set switching mode characteristics
    tacacs-server    Configure TACACS+
    udld             Enable UDLD in the aggressive or normal mode and to set
                     the configurable message timer on all fiber-optic ports.
    username         Establish User Name Authentication
    vlan             VLAN commands
    web              Web
```

Command: Configure Hostname

Syntax: **config hostname**

Description: Configure this system's network name (Hostname).

Mode: (config)#

Example: Change this system's network name (Hostname)

```
(config)# host?
    hostname    Set system's network name
(config)# host word
word(config)#
(config)# hostname ABcd12!@
% Fail to set system configuration.

(config)# hostname ABcd
ABcd(config)# hostname ABcd12
ABcd12(config)# hostname #
                         ^
% Invalid word detected at '^' marker.

ABcd12(config)# hostname 1
                         ^
% Invalid word detected at '^' marker.

ABcd12(config)# hostname A
A(config)# A b
           ^
% Ambiguous word detected at '^' marker.

A(config)# A 1
           ^
% Ambiguous word detected at '^' marker.

A(config)#
```

Configure a Specific Interface

To configure a specific Interface in terms of its possible functions. To enter the configure interface mode:

```
# con ter
(config)# interface ?
    *                    All switches or All ports
    ManagementPort       Management Port
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
    vlan                 VLAN interface configurations
(config)# interface 10GigabitEthernet ?
    <port_type_list>    Port list in 1/1-4
(config)# interface 10GigabitEthernet 1/1-3
(config-if)#
```

The configurable parameters are:

access-list Access list
aggregation Create an aggregation
ddmi Digital Diagnostic Monitoring Interface (rx-power-int-thresh)
description <port_desc>
do To run exec commands in config mode
dot1x IEEE Standard for port-based Network Access Control
duplex Interface duplex
end Go back to EXEC mode
evc Ethernet Virtual Connections
excessive-restart Restart backoff algorithm after 16 collisions (No excessive-restart means discard frame after 16 collisions)
exit Exit from current mode
flowcontrol Traffic flow control.
green-ethernet Green ethernet (Power reduction)
gvrp Enable GVRP on port(s)
help Description of the interactive help system
ip Internet Protocol
ipv6 IPv6 configuration commands
lacp Enable LACP on this interface
link-oam Enable or Disable(when the no keyword is entered) Link OAM on the interface
lldp LLDP configurations.
loop-protect Loop protection configuration on port
mac MAC keyword
media-type Media type.
mtu Maximum transmission unit
mvr Multicast VLAN Registration configuration
no Negate a command or set its defaults
platform platform phy mode (1G mode or WAN mode)
port-security Enable/disable port security per interface.
Ptp Precision time Protocol (1588)
Pvlan Private VLAN
Qos Quality of Service
Rmon Configure Remote Monitoring on an interface
Shutdown Shutdown of the interface.
snmp-server Set SNMP server's configurations
spanning-tree Spanning Tree protocol
speed Configures interface speed. If you use 10, 100, or 1000 keywords with the auto keyword the port will only advertise the specified speeds.
Switchport Switching mode characteristics
Udld UDLD configuration on port(s).

The interface configuration commands are described in the following sections.

Command: Configure an Interface's Duplex/Excessive/FC/MAC/Media/MTU/Speed

Syntax: **(config-if)#**

Description: Configure a specified interface's parameters.

duplex Interface duplex (auto/full/half duplex mode)
excessive-restart Restart backoff algorithm after 16 collisions (No excessive-restart means discard frame after 16 collisions)
flowcontrol Traffic flow control (on / off).
mac MAC keyword. mac address-table learning Port Secure mode.
media-type Media type (RJ-45/SFP/Dual).
mtu Maximum transmission unit (1518-9600 bytes).
speed Configures interface speed. If you use 10, 100, or 1000 keywords, with the auto keyword the port will only advertise the specified speeds.

Mode: (config-if-vlan)#

Example 1:

```
(config)# interface *
 (config-if)# duplex ?
    auto    Auto negotiation of duplex mode.
    full    Forced full duplex.
    half    Forced half duplex.
(config-if)# duplex full ?
    <cr>
(config-if)# excessive-restart ?
    <cr>
(config-if)# flowcontrol ?
    off    Disable flow control.
    on     Enable flow control.
(config-if)# green-ethernet ?
    energy-detect    Enable power saving for ports with no link partner.
    short-reach      Enable power saving for ports which is connect to link partner with short
                     cable.
(config-if)# mac ?
    address-table    MAC table configuration
(config-if)# mac address-table ?
    learning    Port learning mode
(config-if)# mac address-table learning ?
    secure    Port Secure mode
    <cr>
(config-if)# media-type ?
    dual    Dual media interface (cu & fiber interface).
    rj45    rj45 interface (copper interface).
    sfp     sfp interface (fiber interface).
(config-if)# mtu ?
    1518-10056    Maximum frame size in bytes.
(config-if)# speed ?
    10      10Mbps
    100     100Mbps
    1000    1Gbps
    2500    2.5Gbps
    auto    Auto negotiation
(config-if)# speed
```

Command: Configure Interface Switch / Ports

Syntax: **interface** (<port_type> [<plist>])
Description: Configure the interface port parameters.
Mode: (config-if-vlan)#

Example 1: Display the various command options:

```
(config)# interface ?
    *                     All switches or All ports
    GigabitEthernet       1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
    tunnel-tp             MPLS TP Tunnel
    vlan                  VLAN interface configurations
(config)# interface GigabitEthernet ?
    <port_type_list>    Port list in 1/1-6
(config)# interface 10GigabitEthernet ?
    <port_type_list>    Port list in 1/1-2
(config)# interface 10GigabitEthernet
```

Example 2: Configure the 1 Gigabit Ethernet Port:

```
(config)# interface GigabitEthernet 1/1
(config-if)# interface GigabitEthernet 1/1-8 ?
% No such port: GigabitEthernet 1/5

(config-if)# interface GigabitEthernet 1/1-4 ?
(config-if)# interface GigabitEthernet 1/1-4
```

Example 4: Configure the 2.5 Gigabit Ethernet Port:

```
(config)# interface 2 ?
    <port_type_list>    Port list in 1/1-2
(config)# interface 2  1/1 ?
    *                     All switches or All ports
    GigabitEthernet       1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
    <cr>
(config)# interface 2  1/1
```

Command: Configure Interface VLAN

Syntax: **interface vlan** <vlist>

Description: Configure the interface VLAN parameters.

Mode: (config-if-vlan)#

Example 2: Configure interface VLAN

```
(config)# interface vlan?
    vlan    VLAN interface configurations
(config)# interface vlan?
interface vlan <vlist>
(config)# interface vlan 1
(config-if-vlan)# ?
    do      To run exec commands in config mode
    end     Go back to EXEC mode
    exit    Exit from current mode
    help    Description of the interactive help system
    ip      Interface Internet Protocol config commands
    ipv6    IPv6 configuration commands
    no      Negate a command or set its defaults
(config-if-vlan)# ip?
    ip      Interface Internet Protocol config commands
    ipv6    IPv6 configuration commands
(config-if-vlan)# ip ?
    address    Address configuraton
    dhcp       Configure DHCP server parameters
    igmp       Internet Group Management Protocol
(config-if-vlan)# ip address ?
    <ipv4_addr>    IP address
    dhcp           Enable DHCP
(config-if-vlan)# ip address dhcp ?
    fallback    DHCP fallback settings
    <cr>
(config-if-vlan)# ip address dhcp fallback ?
    <ipv4_addr>    DHCP fallback address
(config-if-vlan)# ipv6 ?
    address    Configure the IPv6 address of an interface
    mld        Multicasat Listener Discovery
```

Messages: *W xxrp 00:14:23 64/alloc_gid#167: Warning: Allocation denied. Limit reached. Only 20 simultanious VLAN allowed for group 0*

Meaning: The limit of 20 VLANs per group was reached.

Recovery: 1. Press the Enter key and log in. 2. Delete a VLAN from the group or create a new group.

Example:

```
(config-if-vlan)# ip address 192.168.1.110 255.255.255.0
(config-if-vlan)# W xxrp 00:14:23 64/alloc_gid#167: Warning: Allocation denied.
Limit reached. Only 20 simultanious VLAN allowed for group 0
W xxrp/gvrp 00:14:23 64/vtss_gvrp_registrar_administrative_control2#2155: Warning: port=0,
vid=21, vlan_reg_type=1, max_vlans=20
W xxrp 00:14:23 64/alloc_gid#167: Warning: Allocation denied. Limit reached. Only 20
simultanious VLAN allowed for group 0
W xxrp/gvrp 00:14:23 64/vtss_gvrp_registrar_administrative_control2#2155: Warning: port=0,
vid=22, vlan_reg_type=1, max_vlans=20
W xxrp 00:14:23 64/alloc_gid#167: Warning: Allocation denied. Limit reached. Only 20
simultanious VLAN allowed for group 0
W xxrp/gvrp 00:14:23 64/vtss_gvrp_registrar_administrative_control2#2155: Warning: port=0,
vid=23, vlan_reg_type=1, max_vlans=20

Press ENTER to get started
```

Command: Configure a Specific Interface Switchport

Syntax: (config-if)# **switchport**

Description: Configure a specific interface switchport's parameters:

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

Mode: (config-if)

Example 1: Display the various functions available:

```
(config)# interface ?
    *                     All switches or All ports
    GigabitEthernet       1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
    tunnel-tp             MPLS TP Tunnel
    vlan                  VLAN interface configurations
(config)# interface 10GigabitEthernet ?
    <port_type_list>    Port list in 1/1-2
(config)# interface 10GigabitEthernet 1/1 ?
    *                     All switches or All ports
    GigabitEthernet       1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
    <cr>
(config)# interface 10GigabitEthernet 1/1
(config-if)# switchport ?
    access       Set access mode characteristics of the interface
    forbidden    Adds or removes forbidden VLANs from the current list of
                 forbidden VLANs
    hybrid       Change PVID for hybrid port
    mode         Set mode of the interface
    trunk        Change PVID for trunk port
    vlan         VLAN commands
(config-if)# switchport
```

Example 2: Configure Switchport Access Mode

```
(config-if)# switchport access ?
    vlan    Set VLAN when interface is in access mode
(config-if)# switchport access vlan ?
    <vlan_id>    VLAN ID of the VLAN when this port is in access mode
(config-if)# switchport access vlan 10 ?
    <cr>
(config-if)# switchport access vlan 10
(config-if)#
```

Example 3: Configure Switchport Forbidden VLAN:

```
(config-if)# switchport forbidden ?
    vlan    Add or modify VLAN entry in forbidden table.
(config-if)# switchport forbidden vlan ?
    add       Add to existing list.
    remove    Remove from existing list.
(config-if)# switchport forbidden vlan add ?
    <vlan_list>    VLAN IDs
(config-if)# switchport forbidden vlan add 100 ?
    <cr>
(config-if)# switchport forbidden vlan add 100
(config-if)#
```

Example 4: Configure Switchport Hybrid:

```
(config-if)# switchport h?
    hybrid    Change PVID for hybrid port
(config-if)# switchport hybrid ?
    acceptable-frame-type    Set acceptable frame type on a port
    allowed                  Set allowed VLAN characteristics when interface is
                             in hybrid mode
    egress-tag               Egress VLAN tagging configuration
    ingress-filtering        VLAN Ingress filter configuration
    native                   Set native VLAN
    port-type                Set port type
(config-if)# switchport hybrid
(config-if)# switchport hybrid acc ?
    all         Allow all frames
    tagged      Allow only tagged frames
    untagged    Allow only untagged frames
(config-if)# switchport hybrid allowed ?
    vlan    Set allowed VLANs when interface is in hybrid mode
(config-if)# switchport hybrid egress-tag ?
    all     Tag all frames
    none    No egress tagging
(config-if)# switchport hybrid ingress-filtering ?
    <cr>
(config-if)# switchport hybrid native ?
    vlan    Set native VLAN when interface is in hybrid mode
(config-if)# switchport hybrid port-type ?
    c-port           Customer port
    s-custom-port    Custom Provider port
    s-port           Provider port
    unaware          Port in not aware of VLAN tags.
(config-if)# switchport hybrid port-type
```

Example 5: Configure Switchport Mode unconditionally:

```
(config-if)# switchport m?
    mode    Set mode of the interface
(config-if)# switchport mode ?
    access    Set mode to ACCESS unconditionally
    hybrid    Set mode to HYBRID unconditionally
    trunk     Set mode to TRUNK unconditionally
(config-if)# switchport mode
```

Example 6: Configure Switchport Trunk mode parameters:

```
(config-if)# switchport t?
    trunk    Change PVID for trunk port
(config-if)# switchport trunk ?
    allowed    Set allowed VLAN characteristics when interface is in trunk mode
    native     Set native VLAN
    vlan       Vlan commands
(config-if)# switchport trunk allowed ?
    vlan    Set allowed VLANs when interface is in trunk mode
(config-if)# switchport trunk allowed vlan ?
    <vlan_list>    VLAN IDs of the allowed VLANs when this port is in trunk
                   mode
    add            Add VLANs to the current list
    all            All VLANs
    except         All VLANs except the following
    none           No VLANs
    remove         Remove VLANs from the current list
(config-if)# switchport trunk native ?
    vlan    Set native VLAN when interface is in trunk mode
(config-if)# switchport trunk native vlan ?
    <vlan_id>    VLAN ID of the native VLAN when this port is in trunk mode
(config-if)# switchport trunk vlan ?
    tag    tag parameters
(config-if)# switchport trunk vlan tag ?
    native    tag native vlan
(config-if)# switchport trunk vlan tag native ?
    <cr>
(config-if)# switchport trunk vlan tag native
(config-if)#
```

Example 7: Configure Switchport VLAN commands:

```
(config-if)# switchport v?
    vlan    VLAN commands
(config-if)# switchport vlan ?
    ip-subnet    VCL IP Subnet-based VLAN configuration.
    mac          MAC-based VLAN commands
    mapping      Maps an interface to a VLAN translation group..
    protocol     Protocol-based VLAN commands
(config-if)# switchport vlan ip-subnet ?
    id    id keyword
(config-if)# switchport vlan ip-subnet id ?
    <1-128>    Unique VCE ID for each VCL entry (1-128)
(config-if)# switchport vlan mac ?
    <mac_ucast>    48 bit unicast MAC address: xx:xx:xx:xx:xx:xx
(config-if)# switchport vlan mac 11-22-33-44-55-66 ?
                                 ^
% Invalid word detected at '^' marker.

(config-if)# switchport vlan mac 00-00-00-00-00-00 ?
    vlan    vlan keyword
(config-if)# switchport vlan mac 00-00-00-00-00-00 vlan ?
    <vlan_id>    VLAN ID required for the group to VLAN mapping (Range: 1-4095)
(config-if)# switchport vlan mac 00-00-00-00-00-00 vlan 10 ?
    <cr>
(config-if)# switchport vlan mapping ?
    <group id : 1-7>    Group id
(config-if)# switchport vlan mapping 1 ?
    <cr>
(config-if)# switchport vlan mapping 1
(config-if)# switchport vlan p?
    protocol    Protocol-based VLAN commands
(config-if)# switchport vlan protocol ?
    group    Protocol-based VLAN group commands
(config-if)# switchport vlan protocol group ?
    <word16>    Group Name (Range: 1 - 16 characters)
(config-if)# switchport vlan protocol group A1 ?
    vlan    vlan keyword
(config-if)# switchport vlan protocol group A1 vlan ?
    <vlan_id>    VLAN ID required for the group to VLAN mapping (Range: 1-4095)
(config-if)# switchport vlan protocol group A1 vlan 10 ?
    <cr>
(config-if)# switchport vlan protocol group A1 vlan 10
(config-if)#
```

Command: Configure a Specific Interface Private VLAN (PVLAN)

Syntax: (config-if)# **pvlan**

Description: Configure a specific interface's PVLAN parameters. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed. Private VLANs are based on the source port mask, and there are 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.

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.

Mode: (config-if)

Example 1: Display the various functions available:

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

Example 2: Configure the PVLAN and show the resulting config:

```
(config-if)# pvlan ?
    <range_list>    list of PVLANs. Range is from 1 to number of ports.
    isolation       Port isolation
(config-if)# pvlan i?
    isolation    Port isolation
    <cr>
(config-if)# pvlan isolation ?
    <cr>
(config-if)# pvlan isolation
(config-if)# end
# show pv?
    pvlan    PVLAN configuration
    <cr>
# show pvlan ?
    <range_list>    PVLAN ID to show configuration for
    isolation       show isolation configuration
    <cr>
# show pvlan
PVLAN ID  Ports
--------  --------------------------------------------------------------------------------
1         GigabitEthernet 1/1, GigabitEthernet 1/2, GigabitEthernet 1/3,
          GigabitEthernet 1/4, 10GigabitEthernet 1/1, 10GigabitEthernet 1/2
# show pvlan isolation
Port                              Isolation
--------------------------------  ---------
GigabitEthernet 1/1               Enabled
GigabitEthernet 1/2               Disabled
GigabitEthernet 1/3               Disabled
GigabitEthernet 1/4               Disabled
10GigabitEthernet 1/1            Disabled
10GigabitEthernet 1/2            Disabled
#
```

Command: Configure a Specific Interface SNMP Host Traps

Syntax: (config-if)# **snmp**

Description: Enable a specific interface's SNMP trap events.

Mode: (config-if)

Example 1: Display the various functions available:

```
(config-if)# snmp host bob traps ?
    linkdown    Link down event
    linkup      Link up event
    lldp        LLDP event
    <cr>
(config-if)# snmp host bob traps
```

Example 2: Config snmp host "bob" in terms of its trap event settings and show resulting config:

```
(config-if)# snmp-server host bob traps linkdown linkup lldp
(config-if)# end
# show snmp host bob interface system switch
Trap Global Mode: Enabled
Trap bob (ID:2) is Enabled
Community       :
Destination Host: e2d0:8000:5c:8201::8e:8000
UDP Port        : 45756
Version         : INVALID!
Warm Start         : Enabled
Cold Start         : Enabled
STP                : Enabled
RMON               : Enabled
GigabitEthernet   1/1  Link Up    : Enabled
GigabitEthernet   1/2  Link Up    : Enabled
GigabitEthernet   1/3  Link Up    : Enabled
GigabitEthernet   1/4  Link Up    : Enabled
GigabitEthernet   1/1  Link Down  : Enabled
GigabitEthernet   1/2  Link Down  : Enabled
GigabitEthernet   1/3  Link Down  : Enabled
GigabitEthernet   1/4  Link Down  : Enabled
-- more --, next page: Space, continue: g, quit: ^C
```

Messages: *Trap Global Mode: disabled*

The interface configuration command parameters are:

access-list action { permit | deny }
access-list logging
access-list policy <policy_id>
access-list port-state
access-list rate-limiter <rate_limiter_id>
access-list shutdown
access-list { redirect | port-copy } interface { <port_type> <port_type_id> | (<port_type> [<port_type_list>]) }

aggregation group <v_uint>

ddmi rx-power-int-thresh <0-65535>

description <port_desc> <line255>

do <command> <cr> to run exec commands in config mode

dot1x guest-vlan
dot1x port-control { force-authorized | force-unauthorized | auto | single | multi | mac-based }
dot1x radius-qos
dot1x radius-vlan
dot1x re-authenticate

end <cr> Go back to EXEC mode

evc [update] [**dei** { colored | fixed }] [tag { inner | outer }] [key { double-tag | normal | ip-addr | mac-ip-addr }] [key-advanced { double-tag | normal | ip-addr | mac-ip-addr }] [addr { source | destination }] [addr-advanced { source | destination }] [**l2cp** { [peer <l2cp_peer_list>] [forward <l2cp_forward_list>] [discard <l2cp_discard_list>] }*1]
evc [**update**] [dei { colored | fixed }] [tag { inner | outer }] [key { double-tag | normal | ip-addr | mac-ip-addr }] [key-advanced { double-tag | normal | ip-addr | mac-ip-addr }] [addr { source | destination }] [addr-advanced { source | destination }] [l2cp { [peer <l2cp_peer_list>] [forward <l2cp_forward_list>] [discard <l2cp_discard_list>] }*1]

exit <cr> Exit from current mode

green-ethernet energy-detect <cr>
green-ethernet short-reach <cr>

gvrp <cr> Enable GVRP on port(s)

help <cr> Description of the interactive help system

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

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

lacp <cr> Enable LACP on this interface
lacp key { <v_1_to_65535> | auto }
lacp port-priority <v_1_to_65535>
lacp role { active | passive }
lacp timeout { fast | slow }

link-oam <cr> Enable or Disable (when the no keyword is entered) Link OAM on the interface
link-oam link-monitor frame { [window <error_window>] [threshold <error_threshold>] }*1
link-oam link-monitor frame-seconds { [window <error_window>] [threshold <error_threshold>] }*1
link-oam link-monitor supported
link-oam link-monitor symbol-period { [window <error_window>] [threshold <error_threshold>] }*1
link-oam mib-retrieval supported
link-oam mode { active | passive }
link-oam remote-loopback supported
link-oam variable-retrieve { local-info | remote-info } This feature is not supported yet.

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

loop-protect <cr> Loop protection configuration on port
loop-protect action { [shutdown] [log] }*1
loop-protect tx-mode

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

no Negate a command or set its defaults

platform phy mode { wan | 1g }

port-security <cr> Enable/disable port security per interface.
port-security maximum [<v_1_to_1024>]
port-security violation { protect | trap | trap-shutdown | shutdown }

ptp <clockinst> [internal]
ptp <clockinst> announce { [interval <interval>] [timeout <timeout>] }*1
ptp <clockinst> delay-asymmetry <delay_asymmetry>
ptp <clockinst> delay-mechanism { e2e | p2p }
ptp <clockinst> delay-req interval <interval>
ptp <clockinst> egress-latency <egress_latency>
ptp <clockinst> ingress-latency <ingress_latency>
ptp <clockinst> sync-interval <interval>
ptp pps-delay { { auto master-port interface <port_type> <v_port_type_id> } | {man cable-delay <cable_delay> } }

ptp pps-sync { main-auto | main-man | sub } [pps-phase <pps_phase>] [cable-asy <cable_asy>] [ser-man | ser-auto]

qos cos <cos>
qos dei <dei>
qos dpl <dpl>
qos dscp-classify { zero | selected | any }
qos dscp-remark { rewrite | remap | remap-dp }
qos dscp-translate
qos map cos-tag cos <cos> dpl <dpl> pcp <pcp> dei <dei>
qos map tag-cos pcp <pcp> dei <dei> cos <cos> dpl <dpl>
qos pcp <pcp>
qos policer <rate> [kbps | mbps | fps | kfps] [flowcontrol]
qos queue-policer queue <queue> <rate> [kbps | mbps]
qos queue-shaper queue <queue> <rate> [kbps | mbps] [excess]
qos shaper <rate> [kbps | mbps]
qos storm { unicast | broadcast | unknown } <rate> [fps | kfps | kbps | mbps]
qos tag-remark { pcp <pcp> dei <dei> | mapped }
qos trust dscp
qos trust tag
qos wrr <w0> <w1> <w2> <w3> <w4> <w5>

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

shutdown <cr> Shutdown of the interface.

udld port [aggressive] [message time-interval <v_interval>]

IPv4 Commands and Parameters

The various IPv4 config commands and their parameters are listed below:

(config)# **ip?**

```
  ip      Internet Protocol
  ipmc    IPv4/IPv6 multicast configuration
  ipv6    IPv6 configuration commands
```

(config)# **ip ?**

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

(config)# **ip??**

```
ip arp inspection
ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>
ip arp inspection translate [ interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var> ]
ip arp inspection vlan <in_vlan_list>
ip arp inspection vlan <in_vlan_list> logging { deny | permit | all }
ip dhcp excluded-address <low_ip> [ <high_ip> ]
ip dhcp pool <pool_name>
ip dhcp relay
ip dhcp relay information option
ip dhcp relay information policy { drop | keep | replace }
ip dhcp server
ip dhcp snooping
ip dns proxy
ip domain name { <v_domain_name> | dhcp [ ipv4 | ipv6 ] [ interface vlan <v_vlan_id_dhcp> ] }
ip helper-address <v_ipv4_ucast>
ip http secure-certificate { upload <url_file> [ pass-phrase <pass_phrase> ] | delete | generate { rsa | dsa } }
ip http secure-redirect
ip http secure-server
ip igmp host-proxy [ leave-proxy ]
ip igmp snooping
ip igmp snooping vlan <v_vlan_list>
ip igmp ssm-range <v_ipv4_mcast> <ipv4_prefix_length>
ip igmp unknown-flooding
ip name-server [ <order> ] { <v_ipv4_ucast> | { <v_ipv6_ucast> [ interface vlan<v_vlan_id_static> ] } |
   dhcp [ ipv4 | ipv6 ] [ interface vlan <v_vlan_id_dhcp>] }
ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>
ip routing
ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var><mask_var>
ip ssh
ip verify source
ip verify source translate
```

The IP config commands are described on the following pages.

Command: Configure IPv4

Syntax: **config ip**

Description: Configure the IPv4 parameters.

The IP stack can be configured to act either as a Host or a Router. In Host mode, IP traffic between interfaces will not be routed. In Router mode, traffic is routed between all interfaces.

The system can be configured with zero or more IP interfaces. Each IP interface is associated with a VLAN, and the VLAN represents the IP broadcast domain. Each IP interface may be configured with an IPv4 and/or IPv6 address.

All management interfaces are by default available on all configured IP interfaces. If this is not desirable, then management access filtering must be configured.

The IP address, IP Mask, IP Router can be configured along with a VLAN assigned. The DHCP (for IPv4) Client can be enabled to automatically to obtain an IP address from a DHCP server.

The fallback mechanism is also provided so that the user can enter time period in seconds to obtain a DHCP address. After this fallback timer expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained.

The IP address of the DNS Server in dotted decimal notation can be provided as part of the IP configuration. The IPv4 parameters are:

<**Network Address**> Enter a valid Destination IPv4 address. The default is none.
<**Mask length**> Enter 1 - 32 for IPv4. The default is none.
<**Gateway** > Enter a valid Destination IPv4 address. The default is none.

Mode: (config)#

Example:

```
(config)# ip?
    ip      Internet Protocol
    ipmc    IPv4/IPv6 multicast configuration
    ipv6    IPv6 configuration commands
(config)# ip ?
    arp                 Address Resolution Protocol
    dhcp                Dynamic Host Configuration Protocol
    dns                 Domain Name System
    domain              IP DNS Resolver
    helper-address      DHCP relay server
    http                Hypertext Transfer Protocol
    igmp                Internet Group Management Protocol
    name-server         Domain Name System
    route               Add IP route
    routing             Enable routing for IPv4 and IPv6
    source              source command
    ssh                 Secure Shell
    verify              verify command
(config-if-vlan)# ip address ?
    <ipv4_addr>    IP address
    dhcp           Enable DHCP
(config-if-vlan)# ip address 192.168.1.110 ?
    <ipv4_netmask>    IP netmask
(config-if-vlan)# ip address 192.168.1.110
<ipv4_netmask>
(config-if-vlan)# ip dhcp ?
    server    Enable DHCP server per VLAN
(config-if-vlan)# ip dhcp server ?
    <cr>
(config-if-vlan)#
```

Command: Configure IP ARP Inspection

Syntax: **ip arp inspection**
ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>
ip arp inspection translate [interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>]
ip arp inspection vlan <in_vlan_list>
ip arp inspection vlan <in_vlan_list> logging { deny | permit | all }

Description: Configure the IP ARP (Address Resolution Protocol) Inspection parameters.
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. This feature is used to block such attacks. Only valid ARP requests and responses can go through the S4224.

Mode: (config)

Example:

```
(config)# ip arp inspection ?
    entry        arp inspection entry
    translate    arp inspection translate all entries
    vlan         arp inspection vlan setting
    <cr>
(config)# ip arp inspection entry ?
    interface    arp inspection entry interface config
(config)# ip arp inspection entry interface ?
    GigabitEthernet       1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
(config)# $pection entry int g 1/2 1 10-00-00-00-00-10 192.168.1.30
(config)# ip arp inspection translate ?
    interface    arp inspection entry interface config
    <cr>
(config)# ip arp inspection translate interface ?
    GigabitEthernet       1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
(config)# ip arp inspection vlan ?
    <vlan_list>    arp inspection vlan list
(config)# ip arp inspection vlan 1 ?
    logging    ARP inspection vlan logging mode config
    <cr>
(config)# ip arp inspection vlan 1 logging ?
    all       log all entries
    deny      log denied entries
    permit    log permitted entries
(config)# ip arp inspection vlan 1 logging all
(config-if)# ip arp inspection trust ?
    <cr>
(config)# end
# show ip arp
192.168.1.30 via VLAN1:00-04-75-bd-9c-36
#
```

Messages: *ARP Inspection: the entry already exists in the database.*

Command: Configure IP DHCP (Dynamic Host Configuration Protocol)

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

Description: Configure the DHCP parameters.

excluded-address : Prevent DHCP from assigning certain addresses.

pool : Configure DHCP address pools.

relay : DHCP relay agent configuration. Relay Information Mode enables or disables the DHCP option 82 operation. 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. The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID (always 0 in standalone device) and the last two characters are the port number.

server : Enable DHCP server. The DHCP (for IPv4) Client can be enabled to automatically to obtain an IP address from a DHCP server. A DHCP Server is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP client. **Note**: after power up, the S4224 has DHCP enabled. If a DHCP server is available, the S4224 will obtain an IP address from the DHCP server. If no DHCP server is available, after 70 seconds, the S4224 will fall back to the default IP address of 192.168.0.1/24.

snooping : DHCP Snooping is used to block intruders on the untrusted ports of the S4224 when it tries to intervene by injecting a bogus DHCP (for IPv4) reply packet to a legitimate conversation between the DHCP (IPv4) client and server.

Mode: (config)#

Example 1: Display the various DHCP functions.

```
(config)# ip dhcp ?
    excluded-address    Prevent DHCP from assigning certain addresses
    pool                Configure DHCP address pools
    relay               DHCP relay agent configuration
    server              Enable DHCP server
    snooping            DHCP snooping
(config)# ip dhcp excluded-address ?
    <ipv4_addr>    Low IP address
(config)# ip dhcp excluded-address 10.1.1.10 ?
    <ipv4_addr>    High IP address
    <cr>
(config)# ip dhcp excluded-address 10.1.1.10
(config)# ip dhcp pool ?
    WORD    Pool name in 32 characters
(config)# ip dhcp pool DP2 ?
    <cr>
(config)# ip dhcp pool DP2
```

```
(config-dhcp-pool)# end
# config term
(config)# ip dhcp relay ?
    information    DHCP information option(Option 82)
    <cr>
(config)# ip dhcp relay information ?
    option    DHCP option
    policy    Policy for handling the receiving DHCP packet already include the
              information option
(config)# ip dhcp relay information option ?
    <cr>
(config)# ip dhcp relay information option
(config)# ip dhcp relay information policy ?
    drop       Drop the package when receive a DHCP message that already
               contains relay information
    keep       Keep the original relay information when receive a DHCP message
               that already contains it
    replace    Replace the original relay information when receive a DHCP
               message that already contains it
(config)# ip dhcp server ?
    <cr>
(config)# ip dhcp server
(config)# ip dhcp snooping ?
    <cr>
(config)# ip dhcp snooping
(config)#
```

Messages: *% Low IP addresse can not be larger than high IP address.*

Example 2: Configure DHCP excluded address parameters and show resulting config:

```
(config)# ip dhcp excluded-address ?

    <ipv4_addr>    Low IP address

(config)# ip dhcp excluded-address 123.4.56.7 ?

    <ipv4_addr>    High IP address

    <cr>

(config)# ip dhcp excluded-address 123.4.56.7 124.4.56.8

(config)# end

# show ip dhcp excluded-address

     Low Address      High Address
     ---------------  ---------------
01   123.4.56.7       124.4.56.8

#
```

Example 3: Display the configurable DHCP pool parameters:

```
(config-dhcp-pool)# ?
    broadcast              Broadcast address in use on the client's subnet
    client-identifier      Client identifier
    client-name            Client host name
    default-router         Default routers
    dns-server             DNS servers
    do                     To run exec commands in config mode
    domain-name            Domain name
    end                    Go back to EXEC mode
    exit                   Exit from current mode
    hardware-address       Client hardware address
    help                   Description of the interactive help system
    host                   Client IP address and mask
    lease                  Address lease time
    netbios-name-server    NetBIOS (WINS) name servers
    netbios-node-type      NetBIOS node type
    netbios-scope          NetBIOS scope
    network                Network number and mask
    nis-domain-name        NIS domain name
    nis-server             Network information servers
    no                     Negate a command or set its defaults
    ntp-server             NTP servers
    vendor                 Vendor configuration

(config-dhcp-pool)# broadcast ?
    A.B.C.D    Broadcast IP address
(config-dhcp-pool)# client-identifier ?
    fqdn           FQDN type of client identifier
    mac-address    MAC address type of client identifier
(config-dhcp-pool)# client-name ?
    WORD    Client hsot name in 32 characters
(config-dhcp-pool)# default-router ?
    A.B.C.D    Router's IP address
(config-dhcp-pool)# dns-server ?
    A.B.C.D    Server's IP address
(config-dhcp-pool)# do ?
    LINE    Exec Command
(config-dhcp-pool)# do domain-name ?
    LINE    Exec Command
    <cr>
(config-dhcp-pool)# hardware-address ?
    MAC    Client MAC address
(config-dhcp-pool)# host ?
    A.B.C.D    Network number
(config-dhcp-pool)# lease ?
    <0-365>     Days
    infinite    Infinite lease
(config-dhcp-pool)# netbios-name-server ?
    A.B.C.D    Server's IP address
(config-dhcp-pool)# netbios-node ?
    b-node    Broadcast node
    h-node    Hybrid node
```

```
    m-node    Mixed node
    p-node    Peer-to-peer node
(config-dhcp-pool)# netbios-scope ?
    LINE    Netbios scope identifier, in 128 characters
(config-dhcp-pool)# network ?
    A.B.C.D    Network number
(config-dhcp-pool)# nis-domain-name ?
    <word128>    NIS domain name
(config-dhcp-pool)# nis-server ?
    A.B.C.D    Server's IP address
(config-dhcp-pool)# ntp-server ?
    A.B.C.D    Server's IP address
(config-dhcp-pool)# vendor ?
    class-identifier    Vendor class identifier
(config-dhcp-pool)#
```

Example 4: Configure DHCP ip dhcp relay parameters

```
(config)# ip dhcp relay ?
    information    DHCP information option(Option 82)
    <cr>
(config)# ip dhcp relay information option
(config)# end
# show ip dhcp relay
Switch DHCP relay mode is enabled
Switch DHCP relay server address is 192.168.1.30
Switch DHCP relay information option is enabled
Switch DHCP relay information policy is replace
#
```

Example 5: Configure DHCP server parameters

```
(config)# ip dhcp server ?
    <cr>
(config)# end
# show ip dhcp ?
    detailed            DHCP server
    excluded-address    Excluded IP database
    pool                DHCP pools information
    relay               DHCP relay agent configuration
    server              DHCP server information
    snooping            DHCP snooping
# show ip dhcp server ?
    |              Output modifiers
    binding        DHCP address bindings
    declined-ip    Declined IP address
    statistics     DHCP server statistics
    <cr>
# show ip dhcp server

DHCP server is globally enabled.
  Enabled VLANs are 10-20.

#
```

Example 6: Configure DHCP snooping and display resulting config:

```
(config)# ip dhcp snooping?
    snooping    DHCP snooping
    <cr>
(config)# ip dhcp snooping
(config)# end
# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following
ManagementPort 1/1 trusted
GigabitEthernet 1/1 trusted
GigabitEthernet 1/2 trusted
GigabitEthernet 1/3 untrusted
GigabitEthernet 1/4 untrusted
GigabitEthernet 1/5 trusted
GigabitEthernet 1/6 trusted
GigabitEthernet 1/7 trusted
GigabitEthernet 1/8 trusted
GigabitEthernet 1/9 trusted
GigabitEthernet 1/10 trusted
GigabitEthernet 1/11 trusted
GigabitEthernet 1/12 trusted
GigabitEthernet 1/13 trusted
GigabitEthernet 1/14 trusted
GigabitEthernet 1/15 trusted
GigabitEthernet 1/16 trusted
GigabitEthernet 1/17 trusted
GigabitEthernet 1/18 trusted
GigabitEthernet 1/19 trusted
-- more --, next page: Space, continue: g, quit: ^C
```

S4224 DHCP Configuration

Notes:

1. Software releases supporting DHCP Server: S3290 v 2.1.x and S42240, S4140 v 2.2.x.
2. To configure DHCP server you must have a VLAN interface setup with a valid IP address.
3. DHCP Server does not support addresses that come from a DHCP relay server. It must directly handle relay packets.
4. May have to turn off some DHCP options in the DHCP client. See "**DHCP Options Used.**" below.
5. DHCP works the same on 1G ports as on 10G ports.
6. S3290 DHCP supports multiple DHCP Pools (one Pool for each VLAN on multiple ports).
7. S3290 DHCP supports multiple Pools/VLANs serving addresses on a single port.

DHCP CLI Configuration Process

1. Prevent DHCP from assigning certain addresses (optional) using the **excluded-address** command.
2. Configure DHCP address pools using the **pool** command.
3. Configure DHCP relay agent using the **relay** command.
4. Enable DHCP server using the **server** command.
5. Configure DHCP snooping using the **snooping** command.

IP DHCP Configuration Commands

```
(config)# ip dhcp??
ip dhcp excluded-address <low_ip> [ <high_ip> ]
ip dhcp pool <pool_name>
ip dhcp relay
ip dhcp relay information option
ip dhcp relay information policy { drop | keep | replace }
ip dhcp server
ip dhcp snooping
ip helper-address <v_ipv4_ucast>
(config)#
```

IP DHCP Show Commands

```
# show ip dhcp??
show ip dhcp detailed statistics { server | client | snooping | relay | normal-forward |
combined } [ interface ( <port_type> [ <in_port_list> ] ) ]
show ip dhcp excluded-address
show ip dhcp pool [ <pool_name> ]
show ip dhcp relay [ statistics ]
show ip dhcp server
show ip dhcp server binding <ip>
show ip dhcp server binding [ state { allocated | committed | expired } ] [ type { automatic |
manual | expired } ]
show ip dhcp server declined-ip
show ip dhcp server declined-ip <declined_ip>
show ip dhcp server statistics
show ip dhcp snooping [ interface ( <port_type> [ <in_port_list> ] ) ]
show ip dhcp snooping table
# show ip dhcp server

DHCP server is globally enabled.
  Enabled VLANs are 10-20.
```

```
# show ip dhcp relay ?
    |             Output modifiers
    statistics    Traffic statistics
    <cr>
# show ip dhcp relay
Switch DHCP relay mode is enabled
Switch DHCP relay server address is 192.168.1.30
Switch DHCP relay information option is enabled
Switch DHCP relay information policy is replace
# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following
ManagementPort 1/1 trusted
GigabitEthernet 1/1 trusted
GigabitEthernet 1/2 trusted
GigabitEthernet 1/3 untrusted
GigabitEthernet 1/4 untrusted
GigabitEthernet 1/5 trusted
GigabitEthernet 1/6 trusted
GigabitEthernet 1/7 trusted
GigabitEthernet 1/8 trusted
GigabitEthernet 1/9 trusted
GigabitEthernet 1/10 trusted
GigabitEthernet 1/11 trusted
GigabitEthernet 1/12 trusted
GigabitEthernet 1/13 trusted
GigabitEthernet 1/14 trusted
GigabitEthernet 1/15 trusted
GigabitEthernet 1/16 trusted
GigabitEthernet 1/17 trusted
GigabitEthernet 1/18 trusted
GigabitEthernet 1/19 trusted
-- more --, next page: Space, continue: g, quit: ^C
```

IP DHCP Pool Commands (optional)

```
(config)# ip dhcp pool ?
    <word32>    Pool name in 32 characters
(config)# ip dhcp pool bob ?
    <cr>
(config)# ip dhcp pool bob
(config-dhcp-pool)# ?
    broadcast              Broadcast address in use on the client's subnet
    client-identifier      Client identifier
    client-name            Client host name
    default-router         Default routers
    dns-server             DNS servers
    do                     To run exec commands in config mode
    domain-name            Domain name
    end                    Go back to EXEC mode
    exit                   Exit from current mode
    hardware-address       Client hardware address
    help                   Description of the interactive help system
```

```
    host                    Client IP address and mask
    lease                   Address lease time
    netbios-name-server     NetBIOS (WINS) name servers
    netbios-node-type       NetBIOS node type
    netbios-scope           NetBIOS scope
    network                 Network number and mask
    nis-domain-name         NIS domain name
    nis-server              Network information servers
    no                      Negate a command or set its defaults
    ntp-server              NTP servers
    vendor                  Vendor configuration
(config-dhcp-pool)#
```

Running Config Example

```
line vty 15
207 !
208 ip dhcp pool chris
209  network 1.1.1.0 255.255.255.0
210  broadcast 1.1.1.255
211  default-router 1.1.1.2
212  lease 1 0 0
213  domain-name test
214  dns-server 8.8.8.8
215 !
216 !
217 end
```

DHCP Options Used

Subnet Mask: DHCP option 1. Specify subnet mask of the DHCP address pool.

Lease Time: DHCP option **51**, **58** and **59**. Specify lease time that allows the client to request a lease time for the IP address. If all are 0's, then it means the lease time is infinite.

Domain Name: DHCP option **15**. Specify domain name that client should use when resolving hostname via DNS.

Broadcast Address: DHCP option **28**. Specify the broadcast address in use on the client's subnet.

Default Router: DHCP option **3**. Specify a list of IP addresses for routers on the client's subnet.

DNS Server: DHCP option **6**. Specify a list of Domain Name System name servers available to the client.

NTP Server: DHCP option **42**. Specify a list of IP addresses indicating NTP servers available to the client.

NetBIOS Node Type: DHCP option **46**. Specify NetBIOS node type option to allow Netbios over TCP/IP clients which are configurable to be configured as described in RFC 1001/1002.

NetBIOS Scope: DHCP option **47**. Specify the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002.

NetBIOS Name Server: DHCP option **44**. Specify a list of NBNS name servers listed in order of preference.

NIS Domain Name: DHCP option **40**. Specify the name of the client's NIS domain.

NIS Server: DHCP option **41**. Specify a list of IP addresses indicating NIS servers available to the client.

Client Identifier: DHCP option **61**. Specify client's unique identifier to be used when the pool is the type of host.

Client Name: DHCP option **12**. Specify the name of client to be used when the pool is the type of host.

Vendor i Class Identifier: DHCP option **60**. Specify to be used by DHCP client to optionally identify the vendor type and configuration of a DHCP client. DHCP server will deliver the corresponding option 43 specific information to the client that sends option 60 vendor class identifier.

Vendor i Specific Information: DHCP option **43**. Specify vendor specific information according to option 60 vendor class identifier.

Command: Configure IP DNS (Domain Name System) Proxy

Syntax: **ip dns proxy**

Description: When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.

Mode: (config)#

Example:

```
(config)# ip dns proxy ?
    <cr>
(config)# ip dns proxy
(config)# end
# show ip domain

Current domain name is not configured.
```

Command: Configure IP Domain Name

Syntax: **ip domain name** { <v_domain_name> | dhcp [ipv4 | ipv6] [interface vlan <v_vlan_id_dhcp>] }

Description: Define the default domain name.

Mode: (config)#

Example: Define the default domain name and display the resulting info:

```
(config)# ip domain name?
    name    Define the default domain name
(config)# ip domain name??
ip domain name { <v_domain_name> | dhcp [ ipv4 | ipv6 ] [ interface vlan <v_vlan_id_dhcp> ] }
(config)# ip domain name?
    name    Define the default domain name
(config)# ip domain name bubba ?
    <cr>
(config)# ip domain name bubba
(config)# end
# show ip domain ?
    |       Output modifiers
    <cr>
# show ip domain

Current domain name is bubba (managed by STATIC).
#
```

Command: Configure HTTPS Certificate

Syntax: **ip http secure-certificate** { upload <url> [pass-phrase <pass_phrase>] | delete | generate { rsa | dsa } }

Description: Generate, upload, or delete a secure HTTPS certificate.

upload: <url_file> Uniform Resource Locator. It is a specific character string that constitutes a reference to a resource. Syntax: <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name>.

For example: *tftp://10.10.10.10/new_image_path/new_image.dat,*
http://username:password@10.10.10.10:80/new_image_path/new_image.dat

A valid file name is a text string drawn from alphabet characters (A-Za-z), digits (0-9), dot (.), hyphen (-), and under score (_). The maximum length is 63 and a hyphen must not be the first character. The file name content that only contains '.' is not allowed.

PassPhrase: The pattern to be used for encrypting the certification.

generate { rsa | dsa }: HTTPS can generate two types of certifications (algorithms), either RSA or DSA:

RSA certification: RSA is one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician, had developed an equivalent system in 1973, but it wasn't declassified until 1997.

DSA certification: The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993. Four revisions to the initial specification have been released: FIPS 186-1 in 1996, FIPS 186-2 in 2000, FIPS 186-3 in 2009, and FIPS 186-4 in 2013.

Mode: (config)

Example 1: Show the command options and generate a secure HTTPS certificate.

```
(config)# ip http secure-certificate ?
    delete      Delete HTTPS certificate
    generate    Generate HTTPS certificate
    upload      Upload HTTPS certificate
(config)# ip http secure-certificate?
    secure-certificate    HTTPS certificate
(config)# ip http secure-certificate generate ?
    dsa    Generate HTTPS certificate with DSA
    rsa    Generate HTTPS certificate with RSA
(config)# ip http secure-certificate generate rsa ?
    <cr>
(config)# ip http secure-certificate generate dsa
(config)# ip http secure-certificate generate rsa
(config)# end
# show ip http server secure status
Switch secure HTTP web server is disabled
Switch secure HTTP web redirection is disabled
Switch secure HTTP certificate is presented
#
```

Example 2: Upload an existing secure HTTPS certificate.

```
(config)# ip http secure-certificate upload ?
    <url_file>    Uniform Resource Locator. It is a specific character string
                  that constitutes a reference to a resource. Syntax:
                  <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name>
                  If the following special characters: space
                  !"#$%&'()*+,/:;<=>?@[\]^`{|}~ need to be contained in the
                  input url string, they should have percent-encoded. A valid
                  file name is a text string drawn from alphabet (A-Za-z),
                  digits (0-9), dot (.), hyphen (-), under score(_). The
                  maximum length is 63 and hyphen must not be first character.
                  The file name content that only contains '.' is not allowed.
(config)# ip http secure-certificate upload?
    upload    Upload HTTPS certificate
(config)# ip http secure-certificate upload??
ip http secure-certificate { upload <url_file> [ pass-phrase <pass_phrase> ] | delete |
generate { rsa | dsa } }

(config)#
```

Message: *ERR_CONNECTION_REFUSED* displays and cannot login .
Meaning: You tried to generate a secure DSA certificate using the “ip secure-certificate generate dsa” command. The self-generated DSA HTTPS certificate did not work.
Recovery:
1. Try a different web browser to log in.
2. Try using RSA secrity instead of DSA.
3. Try to log in again.

Command: Configure IP HTTP (Hypertext Transfer Protocol)

Syntax: **ip http secure-redirect** Secure the HTTP web server
ip http secure-server Secure HTTP web redirection

Description: Configure the running HTTPS server.
Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is used to indicate a secure HTTP connection. HTTPS provides authentication and encrypted communication. The S4224 has an embedded web server for managing the device without any additional software.
The web server also provides a secure interface using HTTPS. The validity period will be based on the validity period of the uploaded cert. If using a generated cert, then the HTTPS Certificate's validity period is from Jan. 1, 2010 to Dec. 31, 2029.
By default the servers listen on standard port 80 for HTTP and on standard port 443 for HTTPS.
The HTTPS runs over SSL and you can upload the certificate using the standard TFTP protocol. You can reconfigure the HTTPS server port for security purposes. No password is used for the SSH certificate. Open SSL commands are available for self-signing a certificate.

Mode: (config)#

Example 1: Use the **ip http secure-redirect** command:

```
(config)# ip http?
    http    Hypertext Transfer Protocol
(config)# ip http ?
    secure-redirect    Secure HTTP web redirection
    secure-server      Secure HTTP web server
(config)# ip http?
    http    Hypertext Transfer Protocol
(config)# ip http?
ip http secure-redirect
ip http secure-server
(config)# ip http secure-redirect ?
    <cr>
#
```

Message:

```
Can not enable the secure HTTP web redirection when the secure HTTP web server is disabled.
% (VTSS_RC_ERROR)
```

Possible Certificate Status is:
Switch secure HTTP certificate is presented: The certification is stored in HTTPS' database.
Switch secure HTTP certificate is not presented: No certification is stored in HTTPS' database.
Switch secure HTTP certificate is generating ...: The certification is generating.

Example 2: Use the **ip http secure-server** command and the **no** version to turn off HTTPS:

```
(config)# ip http secure-server ?
    <cr>
(config)# ip http secure-server
 (config)# ip http secure-server
(config)# ip http secure-redirect
(config)# end
# show ip http server secure ?
    status    Status
# show ip http server secure status
Switch secure HTTP web server is enabled
Switch secure HTTP web redirection is enabled
Switch secure HTTP certificate is presented
# con ter
(config)# ip http secure-server ?
    <cr>
(config)# ip http secure-server
(config)# end
# show ip http server secure status
Switch secure HTTP web server is enabled
Switch secure HTTP web redirection is enabled
Switch secure HTTP certificate is presented
# con ter
(config)# no ip http secure-server
(config)# end
# show ip http server secure status
Switch secure HTTP web server is disabled
Switch secure HTTP web redirection is disabled
Switch secure HTTP certificate is presented
#
```

Command: Configure IP IGMP Host Proxy

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

Description: Configure IGMP proxy for leave configuration. The IGMP (Internet Group Management Protocol) communications protocol is 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 is for unicast connections.

```
(config)# ip igmp host-proxy ?
    leave-proxy    IGMP proxy for leave configuration
    <cr>
(config)# ip igmp host-proxy leave-proxy ?
    <cr>
(config)# ip igmp host-proxy leave-proxy?
    leave-proxy    IGMP proxy for leave configuration
    <cr>
(config)# ip igmp host-proxy leave-proxy
(config)#
```

Command: Configure IGMP Snooping

Syntax: **ip igmp snooping**

Description: Configure the IGMP (Internet Group Management Protocol) Snooping parameters. The IGMP (Internet Group Management Protocol) communications protocol is 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 allows more efficient use of resources when supporting uses such as online video.

Mode: (config-if-vlan)#

Example 1:

```
(config-if-vlan)# ip igmp ?
    snooping    Snooping IGMP
(config-if-vlan)# ip igmp snooping ?
    compatibility                   Interface compatibility
    last-member-query-interval      Last Member Query Interval in tenths of seconds
    priority                        Interface CoS priority
    querier                         IGMP Querier configuration
    query-interval                  Query Interval in seconds
    query-max-response-time         Query Response Interval in tenths of seconds
    robustness-variable             Robustness Variable
    unsolicited-report-interval     Unsolicited Report Interval in seconds
    <cr>
(config-if-vlan)# ip igmp snooping compatibility ?
    auto    Compatible with IGMPv1/IGMPv2/IGMPv3
    v1      Forced IGMPv1
    v2      Forced IGMPv2
    v3      Forced IGMPv3
(config-if-vlan)# ip igmp snooping last-member-query-interval ?
    <IpmcLmqi : 0-31744>    0 - 31744 tenths of seconds
(config-if-vlan)# ip igmp snooping priority ?
    <CosPriority : 0-7>    CoS priority ranges from 0 to 7
(config-if-vlan)# ip igmp snooping querier ?
    address     IGMP Querier address configuration
    election    Act as an IGMP Querier to join Querier-Election
(config-if-vlan)# ip igmp snooping query
query-interval          query-max-response-time
 (config-if-vlan)# ip igmp snooping robustness-variable ?
    <IpmcRv : 1-255>    Packet loss tolerance count from 1 to 255
(config-if-vlan)# ip igmp snooping unsolicited-report-interval
% Incomplete command.

(config-if-vlan)# ip igmp snooping unsolicited-report-interval ?
    <IpmcUri : 0-31744>    0 - 31744 seconds
(config-if-vlan)# ip igmp snooping unsolicited-report-interval
```

Messages: *% Invalid IGMP VLAN 10!*

Command: Configure IGMP Snooping VLAN

Syntax: **ip igmp snooping vlan**
Description: Configure the IGMP Snooping VLAN parameters.
Mode: (config)#
Example 1:

```
(config)# ip igmp snooping vlan ?
    <vlan_list>    VLAN identifier(s): VID
(config)# ip igmp snooping vlan?
    vlan    IGMP VLAN
(config)# ip igmp snooping vlan?
ip igmp snooping vlan <v_vlan_list>
(config)# ip igmp snooping vlan ?
    <vlan_list>    VLAN identifier(s): VID
(config)# ip igmp snooping vlan 1 ?
    <cr>
(config)# ip igmp snooping vlan 1
(config)#
```

Command: Configure IGMP SSM Range

Syntax: **ip igmp ssm-range** <v_ipv4_mcast> <ipv4_prefix_length>
Description: Configure the IGMP SSM (Source Specific Multicast) parameters.
Mode: (config)#
Example: Display the command functions:

```
(config)# ip igmp ssm-range?
    ssm-range    IPv4 address range of Source Specific Multicast
(config)# ip igmp ssm-range?
ip igmp ssm-range <v_ipv4_mcast> <ipv4_prefix_length>
(config)# ip igmp ssm-range 224.20.10.221 ?
    <4-32>    Prefix length ranges from 4 to 32
(config)# ip igmp ssm-range 224.20.10.221 6 ?
    <cr>
(config)# ip igmp ssm-range 224.20.10.221 6
(config)#
```

Command: Configure IGMP Unknown Flooding

Syntax: **ip igmp unknown-flooding**
Description: Configure the IGMP Flooding unregistered IPv4 multicast traffic.
Mode: (config)#
Example: Display the command functions:

```
(config)# ip igmp unknown-flooding ?
    <cr>
(config)# ip igmp unknown-flooding?
    unknown-flooding    Flooding unregistered IPv4 multicast traffic
    <cr>
(config)# ip igmp unknown-flooding
(config)#
```

Messages: *IGMP Snooping is disabled to stop snooping IGMP control plane.*
IGMP Snooping is disabled to stop snooping IGMP control plane.
Multicast streams destined to unregistered IGMP groups will be flooding.

Command: Configure IP DNS (Domain Name System) Name Server

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

Description: Configure IP DNS (Domain Name System) parameters.

Mode: (config)#

Example 1: Configure IP DNS parameters:

```
(config)# ip name-server ?
    <0-3>           Preference of DNS server; Default selection is 0
    <ipv4_ucast>    A valid IPv4 unicast address
    <ipv6_ucast>    A valid IPv6 unicast address
    dhcp            Dynamic Host Configuration Protocol
(config)# ip name-server 0 ?
    <ipv4_ucast>    A valid IPv4 unicast address
    <ipv6_ucast>    A valid IPv6 unicast address
    dhcp            Dynamic Host Configuration Protocol
(config)# ip name-server 0 1?
    <ipv4_ucast>    A valid IPv4 unicast address
    <ipv6_ucast>    A valid IPv6 unicast address
(config)# ip name-server 10.10.10.100 ?
    <cr>
(config)# ip name-server 10.10.10.100
(config)# ip name-server 220.10.20.200 ?
    <cr>
(config)# ip name-server 220.10.20.200
(config)# ip name-server ?
    <0-3>           Preference of DNS server; Default selection is 0
    <ipv4_ucast>    A valid IPv4 unicast address
    <ipv6_ucast>    A valid IPv6 unicast address
    dhcp            Dynamic Host Configuration Protocol
(config)# ip name-server dhcp ?
    interface    Select an interface to configure
    ipv4         DNS setting is derived from DHCPv4; Default selection
    ipv6         DNS setting is derived from DHCPv6
    <cr>
(config)# ip name-server dhcp interface ?
    vlan    VLAN Interface
(config)# ip name-server dhcp interface vlan ?
    <vlan_id>    VLAN identifier(s): VID
(config)# ip name-server dhcp interface vlan 10 ?
    ipv4    DNS setting is derived from DHCPv4; Default selection
    ipv6    DNS setting is derived from DHCPv6
    <cr>
(config)# ip name-server dhcp interface vlan 10
(config)#
```

Command: Enable IP Routing / Configure IP Route for IPv4 and IPv6

Syntax: ***ip route*** Add an IP route
ip routing Enable routing for IPv4 and IPv6

Description: Enable IP Routing and configure the IPv4 / IPv6 Routing parameters. S4224 Static routing provides the ability to route IPv4 and IPv6 frames between different VLANs. These VLANs may or may not exist on different ports, and in a stacking scenario they may exist on different nodes.

The S4224 acts as a router by default. If the device has hardware routing capabilities, those will be used, otherwise routing will be done in software. Whenever an IP interface is configured, the corresponding interface route will be installed in the routing table. Besides from the interfaces routes, the administrator of the device can install static routes into the routing table.

Mode: (config)#

Example 1:

```
(config)# ip routing?
    routing    Enable routing for IPv4 and IPv6
    <cr>
(config)# ip routing ?
    <cr>
(config)# ip routing
(config)# ip route ?
    <ipv4_addr>    Network
(config)# ip route 192.168.1.110 ?
    <ipv4_netmask>    Netmask
(config)# ip route 192.168.1.110 255.255.255.0 ?
    <ipv4_gateway>    Gateway
(config)# ip route 192.168.1.110 255.255.255.0 192.168.1.10 ?
    <cr>
(config)# ip route 192.168.1.110 255.255.255.0 192.168.1.10
(config)#
```

Messages: *% Failed to add route.* displays if you enter the **ip route** command before you enable IP routing via the **ip routing** command. Also try configuring VLAN 1 IP address and mask:

```
(config)# int vlan 1
(config-if-vlan)# ip addr 192.168.1.110 255.255.255.0
(config-if-vlan)# end
# copy running-config start
```

Command: Configure IP Source Binding Interface

Syntax: **ip source binding interface** <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mac_var>

Description: IP Source Guard is a security feature used to restrict IP traffic on DHCP snooping untrusted ports by manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof using the IP address of another host.

Mode: (config)#

Example: Configure an ip source binding interface and display resulting config:

```
(config)# ip source ?
    binding    ip source binding
(config)# ip source binding ?
    interface    ip source binding entry interface config
(config)# ip source binding interface ?
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
(config)# ip source binding interface GigabitEthernet ?
    <port_type_id>    Port ID in 1/1-24
(config)# ip source binding interface GigabitEthernet 1/1 ?
    <vlan_id>    Select a VLAN id to configure
(config)# ip source binding interface GigabitEthernet 1/1 10 ?
    <ipv4_ucast>    Select an IP Address to configure
(config)# ip source binding interface GigabitEthernet 1/1 10 192.168.1.30 ?
    <ipv4_netmask>    Select a subnet mask to configure
(config)# $terface GigabitEthernet 1/1 10 192.168.1.30 255.255.255.0 ?
    <cr>
(config)# $terface GigabitEthernet 1/1 10 192.168.1.30 255.255.255.0
(config)# end
# show ip source binding

Type     Port                    VLAN  IP Address       IP Mask
----     ----                    ----  ----------       -------
Static   GigabitEthernet 1/1       10  192.168.1.30     255.255.255.0
#
```

Command: Configure IP Verify Source / Translate

Syntax: **ip verify source**
ip verify source translate
Description: Verify the IP source binding and tranlate dynamic entries into static entries.
Mode: (config)
Example: Translate dynamic entries into static entries.

```
 (config)# ip verify ?
    source    verify source
(config)# ip verify source ?
    translate    ip verify source translate all entries
    <cr>
(config)# ip verify source
(config)# ip verify source translate ?
    <cr>
(config)# ip verify source translate
IP Source Guard:
        Translate 0 dynamic entries into static entries.
(config)#
```

Command: Configure IP SSH

Syntax: **ip ssh**
ip verify source translate
Description: Enable or disable SSH. SSH (Secure SHel) is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The default is SSH disabled.
Mode: (config)
Example: Enable or disable SSH and display resulting config:

```
# show ip ssh
Switch SSH is enabled
# con ter
(config)# no ip ssh
(config)# end
# show ip ssh
Switch SSH is disabled
#
```

Command: Configure IPMC

Syntax: **ipmc profile**
ipmc profile <profile_name>
ipmc range <entry_name> { <v_ipv4_mcast> [<v_ipv4_mcast_1>] | <v_ipv6_mcast> [<v_ipv6_mcast_1>] }

Description: Configure IPMC (IP Multimedia Communications) . The IPMC commands provide Multicast Listener Discovery (MLD) and Internet Group Management Protocol (IGMP) snooping functions. IPMC 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.

Mode: (config)#

Example:

```
(config)# ipmc profile range?
    <word16>    Profile name in 16 char's
    <cr>
(config)# ipmc ?
    profile    IPMC profile configuration
    range      A range of IPv4/IPv6 multicast addresses for the profile
(config)# ipmc profile ?
    <word16>    Profile name in 16 char's
    <cr>
(config)# ipmc profile sam
(config-ipmc-profile)# ?
    default        Set a command to its defaults
    description    Additional description about the profile in 64 char's
    do             To run exec commands in config mode
    end            Go back to EXEC mode
    exit           Exit from current mode
    help           Description of the interactive help system
    no             Negate a command or set its defaults
    range          A range of IPv4/IPv6 multicast addresses for the
                   profile
(config-ipmc-profile)# end
# show ipmc ?
    profile    IPMC profile configuration
    range      A range of IPv4/IPv6 multicast addresses for the profile
# show ipmc profile ?
    |           Output modifiers
    <word16>    Profile name in 16 char's
    detail      Detail information of a profile
    <cr>
# show ipmc profile

IPMC Profile is currently disabled, please enable profile to start
filtering.

Profile: sam (In VER-INI Mode)
Description:
# show ipmc profile detail

IPMC Profile is currently disabled, please enable profile to start
filtering.

Profile: sam (In VER-INI Mode)
```

```
Description:

IGMP will deny matched address between [224.0.0.0 <-> 239.255.255.255]
MLD will deny matched address between [ff00:: <->
ffff:ffff:ffff:ffff:ffff:ffff:
ffff:ffff]
# show ipmc range ?
    |           Output modifiers
    <word16>    Range entry name in 16 char's
    <cr>
# show ipmc range
#
```

Messages: *% Invalid range name R01.*

Command: Configure IPv6 MLD (Multicast Listener Discovery)

Syntax: **ipv6 mld host-proxy** [leave-proxy]
ipv6 mld snooping
ipv6 mld snooping vlan <v_vlan_list>
ipv6 mld ssm-range <v_ipv6_mcast> <ipv6_prefix_length>
ipv6 mld unknown-flooding

Description: Configure IPv6 MLD (Multicast Listener Discovery) parameters.

Mode: (config)#

Example 1:

```
(config)# ipv6 ?
    mld                Multicasat Listener Discovery:
    host-proxy          MLD proxy configuration
    snooping            Snooping MLD
    ssm-range           IPv6 address range of Source Specific Multicast
    unknown-flooding    Flooding unregistered IPv6 multicast traffic
    route                 Configure static routes:
                         X:X:X:X::X/<0-128>    IPv6 prefix x:x::y/z
(config)# ipv6
```

Example 2:

```
(config)# ipv6 ?
    mld      Multicasat Listener Discovery
    route    Configure static routes
(config)# ipv6?
    ipv6    IPv6 configuration commands
(config)# ipv6??
ipv6 mld host-proxy [ leave-proxy ]
ipv6 mld snooping
ipv6 mld snooping vlan <v_vlan_list>
ipv6 mld ssm-range <v_ipv6_mcast> <ipv6_prefix_length>
ipv6 mld unknown-flooding
ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6
_addr> }
(config)# ipv6
```

Example 3:

```
(config)# ipv6 mld host-proxy ?
    leave-proxy    MLD proxy for leave configuration
    <cr>
(config)# ipv6 mld snooping ?
    vlan    MLD VLAN
    <cr>
(config)# ipv6 mld snooping vlan ?
    <vlan_list>    VLAN identifier(s): VID
(config)# ipv6 mld ssm-range ?
    <ipv6_mcast>    Valid IPv6 multicast address
(config)# ipv6 mld unknown-flooding ?
    <cr>
(config)# ipv6 mld unknown-flooding
```

Example 4:

```
(config)# ipv6 route 222:222:1:1::1/2 ?
    X:X:X:X::X    IPv6 unicast address (except link-local address) of next-hop
    interface     Select an interface to configure
(config)# ipv6 route 222:222:1:1::1/2 110:10:10:10::10 ?
    <cr>
(config)# ipv6 route 222:222:1:1::1/2 110:10:10:10::10
(config)#
```

Command: Configure IPv6 Static Routes

Syntax: **ipv6 route** <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> }

Description: Configure IPv6 static routing. Static routing provides the ability to route IPv4 and IPv6 frames between different VLANs. These VLANs may or may not, exists on different ports, and in a stacking scenario they may exists on different nodes. The device acts as a router by default. If the device has hardware routing capabilities, those will be used, otherwise routing will be done in software. Whenever an IP interface is configured, the corresponding interface route will be installed in the routing table.
Aside from the interfaces routes, the device administrator can also install static routes into the routing table.
VLAN IP Interface configuration parameters are available for assigning an IP address corresponding to a VLAN.

Mode: (config)#

Example 1: Display the command functions and config:

```
(config)# ipv6 route?
    route    Configure static routes
(config)# ipv6 route??
ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6
_addr> }
(config)# ipv6 route ?
    <ipv6_subnet>    IPv6 prefix x:x::y/z
(config)# ipv6 route 1:1::1/2 ?
    X:X:X:X::X    IPv6 unicast address (except link-local address) of next-hop
    interface     Select an interface to configure
(config)# ipv6 route 1:1::1/2?
    X:X:X:X::X/<0-128>    IPv6 prefix x:x::y/z
(config)# ipv6 route 1:1::1/2 ?
    X:X:X:X::X    IPv6 unicast address (except link-local address) of next-hop
    interface     Select an interface to configure
(config)# ipv6 route 1:1::1/2 interface ?
    vlan    VLAN Interface
(config)# ipv6 route 1:1::1/2 interface vlan ?
    <vlan_id>    VLAN identifier(s): VID
(config)# ipv6 route 1:1::1/2 interface vlan 10 ?
    FE80::X:X:X    IPv6 link-local address of next-hop
(config)# ipv6 route 1:1::1/2 interface vlan 10
```

Command: Configure IPv6 Address

Syntax: **ipv6 address**

Description: Configure the IPv6 address of an interface.

Mode: (config)#

Example: Configure the IPv6 address of an interface and display the resulting config:

```
(config-if-vlan)# ipv6 address 2001:db8:a::123/64
(config-if-vlan)# end
# show ipv6 route
::1/128 via ::1 <UP HOST>
2001:db8:a::/64 via VLAN2 <UP HW_RT>
2001:db8:a::123/128 via c0:f256:1a90:: <UP HOST>
#
```

Example: Configure the IPv6 address and enable DHCP Client:

```
(config-if-vlan)# ipv6 address ?
    <ipv6_subnet>    IPv6 prefix x:x::y/z
    dhcp             Enable DHCPv6 client function
(config-if-vlan)# ipv6 address dhcp ?
    rapid-commit    Enable DHCPv6 client Rapid-Commit option
    <cr>
(config-if-vlan)# ipv6 address dhcp rapid-commit ?
    <cr>
(config-if-vlan)# ipv6 address dhcp rapid-commit
(config-if-vlan)#
```

Messages: *% Invalid word detected at '^' marker.*

```
(config-if-vlan)# ipv6 address ?
    X:X:X:X::X/<0-128>    IPv6 prefix x:x::y/z
(config-if-vlan)# ipv6 address 192.168.1.30::10/10 ?
                              ^
% Invalid word detected at '^' marker.
```

Command: Configure IPv6 MLD Snooping

Syntax: **ipv6 mld snooping**
Description: Configure IPv6 Multicast Listener Discovery.
Mode: (config)
Example: Display the command functions and config:

```
(config-if-vlan)# ipv6 mld snooping ?
    compatibility                 Interface compatibility
    last-member-query-interval    Last Member Query Interval in tenths of seconds
    priority                      Interface CoS priority
    querier                       MLD Querier configuration
    query-interval                Query Interval in seconds
    query-max-response-time       Query Response Interval in tenths of seconds
    robustness-variable           Robustness Variable
    unsolicited-report-interval   Unsolicited Report Interval in seconds
    <cr>
(config-if-vlan)# ipv6 mld snooping compatibility ?
    auto    Compatible with MLDv1/MLDv2
    v1      Forced MLDv1
    v2      Forced MLDv2
(config-if-vlan)# ipv6 mld snooping last-member-query-interval ?
    <IpmcLmqi : 0-31744>    0 - 31744 tenths of seconds
(config-if-vlan)# ipv6 mld snooping priority ?
    <CosPriority : 0-7>    CoS priority ranges from 0 to 7
(config-if-vlan)# ipv6 mld snooping querier ?
    election    Act as a MLD Querier to join Querier-Election
(config-if-vlan)# ipv6 mld snooping querier election ?
    <cr>
 (config-if-vlan)# ipv6 mld snooping query-interval ?
    <IpmcQi : 1-31744>    1 - 31744 seconds
(config-if-vlan)# ipv6 mld snooping query-max-response-time ?
    <IpmcQri : 0-31744>    0 - 31744 tenths of seconds
(config-if-vlan)# ipv6 mld snooping robustness-variable ?
    <IpmcRv : 1-255>    Packet loss tolerance count from 1 to 255
(config-if-vlan)# ipv6 mld snooping unsolicited-report-interval ?
    <IpmcUri : 0-31744>    0 - 31744 seconds
(config-if-vlan)# ipv6 mld snooping unsolicited-report-interval
```

IPv6 MLD Snooping Parameters

Configurable Parameter	Valid Range	Default
VLAN ID	1 to 4095	None
Snooping	Enabled Enabled (up to 32VLANs)/Disabled	Disabled
IGMP Querier	Enabled/Disabled	Enabled
Querier address	A valid IP Address	0.0.0.0
Compatibility	IGMP-Auto, Forced IGMPv1,Forced IGMPv2, Forced IGMPv3	IGMP-Auto
Compatibility (MLD)	MLD-Auto, Forced MLDv1, Forced MLDv2/MLD-Auto	MLD-Auto
Priority	0 to 7	0
Robustness Variable	1 to 255	2
Query Interval	1 to 31744 in seconds	125 seconds
Query Response Interval	0 to 31744 in tenths of seconds	100 (=10 sec)
Last Member Query Interval	0 to 31744 in tenths of seconds	10 (= 1 sec)
Unsolicited Report Interval	0 to 31744 in seconds	1 second

Command: Configure DHCPv6 Client Service

Syntax: **dhcp-client**

Description: Configure DHCPv6 client service. Restart a DHCPv6 client service.

Mode: (config)

Example: Display the various dhcp-client command functions:

```
# ipv6?
ipv6 dhcp-client restart [ interface vlan <v_vlan_list> ]
# ipv6 dhcp-client
restart
# ipv6 dhcp-client restart?
    restart    Retart DHCPv6 client service
    <cr>
# ipv6 dhcp-client restart?
ipv6 dhcp-client restart [ interface vlan <v_vlan_list> ]
# ipv6 dhcp-client restart interface ?
    vlan    VLAN of IPv6 interface
# ipv6 dhcp-client restart interface vlan ?
    <vlan_list>    IPv6 interface VLAN list
# ipv6 dhcp-client restart interface vlan 10
#
```

Messages:

 # ipv6 dhcp-client restart interface vlan 10

% Invalid DHCPv6 client interface Vlan10

Command: Configure LACP

Syntax: **lacp system-priority** <v_1_to_65535>

Description: Configure LACP system settings. LACP is the IEEE 802.3ad Link Aggregation Control Protocol that allows bundling several physical ports together to form a single logical port.

The S4224 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 S4224 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, then the flows belonging to that link are transferred to another link based on the hash mechanism which will then choose from the available links. The *static* aggregation option is also supported so the S4224 will work with devices which don't support LACP.

Note: The LACP module can have up to four groups, and up to eight ports can be in a LAG (Link Aggregation Group) at any time. For GLAGs, port speed must match group speed and duplex must be full.

Mode: (config)#

Example 1:

```
(config)# lacp sys ?
    <1-65535>    Priority value; lower means higher priority.
(config)# lacp system-priority 1
(config)# end
# show lacp system-id
System Priority: 1
```

Example 2:

```
# show lacp internal
Port                  Mode      Key   Role    Timeout  Priority
--------------------  --------  ----  ------  -------  --------
Gi 1/1                Disabled  Auto  Active  Fast     32768
Gi 1/2                Disabled  Auto  Active  Fast     32768
Gi 1/3                Disabled  Auto  Active  Fast     32768
Gi 1/4                Disabled  Auto  Active  Fast     32768
2.5G 1/1              Disabled  Auto  Active  Fast     32768
2.5G 1/2              Disabled  Auto  Active  Fast     32768
# show lacp neighbour ?
    |       Output modifiers
    <cr>
# show lacp neighbour
# show lacp statistics ?
    |       Output modifiers
    <cr>
# show lacp statistics
# show lacp system-id ?
    |       Output modifiers
    <cr>
# show lacp system-id
System Priority: 2
```

Command: Configure Line

Syntax: **line** { <0~16> | console 0 | vty <0~15> }

Description: Configure a terminal line.

Mode: (config)#

Example 1:

```
(config)# line ?
    <0~16>     List of line numbers
    console    Console terminal line
    vty        Virtual terminal
(config)# line
    0    Console Line number
w(config)# line vty ?
line { <0~16> | console 0 | vty <0~15> }
(config)# line 9 ?
    <cr>
(config)# line 9
(config-line)# ?
    do              To run exec commands in config mode
    editing         Enable command line editing
    end             Go back to EXEC mode
    exec-banner     Enable the display of the EXEC banner
    exec-timeout    Set the EXEC timeout
    exit            Exit from current mode
    help            Description of the interactive help system
    history         Control the command history function
    length          Set number of lines on a screen
    location        Enter terminal location description
    motd-banner     Enable the display of the MOTD banner
    no              Negate a command or set its defaults
    privilege       Change privilege level for line
    width           Set width of the display terminal
(config-line)# exit
```

Example 2:

```
(config)# line console?
    console    Console terminal line
(config)# line console ?
    0    Console Line number
 (config)# line console 0
(config-line)# ?
    do              To run exec commands in config mode
    editing         Enable command line editing
    end             Go back to EXEC mode
    exec-banner     Enable the display of the EXEC banner
    exec-timeout    Set the EXEC timeout
    exit            Exit from current mode
    help            Description of the interactive help system
    history         Control the command history function
    length          Set number of lines on a screen
    location        Enter terminal location description
    motd-banner     Enable the display of the MOTD banner
    no              Negate a command or set its defaults
    privilege       Change privilege level for line
    width           Set width of the display terminal
(config-line)#
```

Example 3:

```
(config)# line vty?
    vty    Virtual terminal
(config)# line vty?
line { <0~16> | console 0 | vty <0~15> }
(config)# line vty?
    vty    Virtual terminal
(config)# line vty 1 ?
    <cr>
(config)# line vty 1?
    <0~15>    List of vty numbers
    <cr>
(config)# line vty 1
(config-line)# ?
    do              To run exec commands in config mode
    editing         Enable command line editing
    end             Go back to EXEC mode
    exec-banner     Enable the display of the EXEC banner
    exec-timeout    Set the EXEC timeout
    exit            Exit from current mode
    help            Description of the interactive help system
    history         Control the command history function
    length          Set number of lines on a screen
    location        Enter terminal location description
    motd-banner     Enable the display of the MOTD banner
    no              Negate a command or set its defaults
    privilege       Change privilege level for line
    width           Set width of the display terminal
(config-line)#
```

Command: Configure LLDP

Syntax: **lldp holdtime** <val>
lldp reinit <val>
lldp med <val>
lldp timer <val>
lldp transmission-delay <val>

Description: Configure LLDP parameters. LLDP (Link Layer Discovery Protocol) helps network administrators manage the network and maintain an accurate network topology. LLDP capable devices discover each other by periodically advertising their presence and configuration parameters via messages called *Type Length Value* (TLV) fields to neighbor devices. The LLDP configurable parameters are:

holdtime Sets LLDP hold time (the neighbor switch discards the LLDP info after "hold time" multiplied by "timer" seconds). The valid range is 2-10 seconds. The default is 4 seconds.

med Media Endpoint Discovery, an LLDP enhancement, known as LLDP-MED.

reinit The LLDP tx reinitialization delay in seconds. The valid range is 1-10 seconds. The default is 4 seconds.

timer Sets LLDP TX interval (the time between each LLDP frame transmitted in seconds). The valid range is 5-32768 seconds. The default is 30 seconds.

transmission-delay Sets LLDP transmision-delay. LLDP transmission delay (the amount of time that the transmission of LLDP frames will delayed after LLDP configuration has changed) in seconds. The valid range is 1-8192 seconds.The default is 2 seconds.

Mode: (config)#

Example: Configure LLDP parameters:

```
(config)# lldp holdtime ?
    <2-10>    2-10 seconds.
(config)# lldp holdtime 2 ?
    <cr>
(config)# lldp holdtime 2
(config)# lldp reinit ?
    <1-10>    1-10 seconds.
(config)# lldp reinit 2
 (config)# lldp timer ?
    <5-32768>    5-32768 seconds.
(config)# lldp timer 16
(config)# lldp transmission-delay ?
    <1-8192>    1-8192 seconds.
(config)# lldp transmission-delay 8000
(config)#
```

Messages: *According to IEEE 802.1AB-clause 10.5.4.2, the transmission-delay must not be larger than LLDP timer * 0.25. LLDP timer changed to 8000*

LLDP Med Parameters

This function applies to VoIP devices which support LLDP-MED. See the S4224 Web Interface User Guide or the online Help for more information.

datum Datum (geodetic system) type.
fast Number of times to repeat LLDP frame transmission at fast start.
location-tlv LLDP-MED Location Type Length Value parameter.
media-vlan-policy Use the media-vlan-policy to create a policy, which be assigned to an interface.

lldp med datum { wgs84 | nad83-navd88 | nad83-mllw }
lldp med fast <v_1_to_10>
lldp med location-tlv altitude { meters | floors } <v_word11>
lldp med location-tlv civic-addr { country | state | county | city | district |block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code } <v_line>
lldp med location-tlv elin-addr <v_word25>
lldp med location-tlv latitude { north | south } <v_word8>
lldp med location-tlv longitude { west | east } <v_word9>
lldp med media-vlan-policy <policy_index> { voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling } { tagged <v_vlan_id> | untagged } [l2-priority <v_0_to_7>] [dscp <v_0_to_63>]

civic-addr: Civic address information and postal information. The total number of characters for the combined civic address information must not exceed 250 characters. Note: 1) A non empty civic address location will use 2 extra characters in addtion to the civic address location text. 2) The 2 letter country code is not part of the 250 characters limitation.

elin-addr: Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling. Emergency Location Identification Number, (e.g. E911 and others), such as defined by TIA or NENA.

Policy ID (0-31) for the policy which is created:
guest-voice Create a guest voice policy.
guest-voice-signaling Create a guest voice signaling policy.
softphone-voice Create a softphone voice policy.
streaming-video Create a streaming video policy.
video-conferencing Create a video conferencing policy.
video-signaling Create a video signaling policy.
voice Create a voice policy.
voice-signaling Create a voice signaling policy.

lldp med media-vlan-policy <policy_index> { voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-vid eo | video-signaling } { untagged | tagged v_vlan_id> [l2-priority <v_0_to_7>] } [dscp <v_0_to_63>]

Command: Configure Logging

Syntax: **config logging**

Description: Configure System logging (Syslog) parameters. Syslog is a method to collect messages from devices to a server running a Syslog daemon. Logging to a central Syslog server helps in aggregation of logs and alerts. The S4224 can send the log messages to a configured Syslog server running on UDP Port 512. The maximum number of buffered Logs is based on Log message length and is limited to total stored size of 10K.

Mode: (config)#

Example: Display the log commands:

```
(config)# logging ?
    host     host
    level    Severity level
    on       Enable Switch logging host mode
(config)# logging host ?
    <domain_name>    The domain name is to provide a mechanism for naming
                     resources on the Internet. A complete domain name consists
                     of one or more subdomain names which are separated by
                     dots(.)
    <ipv4_ucast>     The IPv4 address of the log server
(config)# logging level ?
    error            Severity 3: Error conditions
    informational    Severity 6: Informational messages
    notice           Severity 5: Normal but significant condition
    warning          Severity 4: Warning conditions
(config)# logging on ?
    <cr>
(config)# end
# show logging ?
    <1-4294967295>    Logging ID
    |                 Output modifiers
    error             Severity 3: Error conditions
    informational     Severity 6: Informational messages
    notice            Severity 5: Normal but significant condition
    warning           Severity 4: Warning conditions
    <cr>
# show logging
Switch logging host mode is enabled
Switch logging host address is null
Switch logging level is informational

Number of entries on Switch 1:
Error        : 1
Warning      : 0
Notice       : 7
Informational: 1
All          : 9

ID          Level          Time & Message
----------  -------------  --------------
         1  Error          1970-01-01T00:00:01+00:00
                           Exception 2 caught at PC 0x801e2210 - TLB miss (Load
                            or IFetch)

         2  Informational  1970-01-01T00:00:02+00:00
                           SYS-BOOTING: Switch just made a cool boot.

         3  Notice         1970-01-01T00:00:02+00:00
                           LINK-UPDOWN: Interface Vlan 1, changed state to down
-- more --, next page: Space, continue: g, quit: ^C
```

Syslog Parameters

Logging Host Descriptions

Logging Host	Description
<domain_name>	The domain name provides a mechanism for naming resources on the Internet. A complete domain name consists of one or more subdomain names which are separated by dots (.).
<ipv4_ucast>	The IPv4 address of the log server.

Logging Level Descriptions

Logging Level	Description
error	Severity 3: Error conditions.
informational	Severity 6: Informational messages.
notice	Severity 5: Normal but significant condition.
warning	Severity 4: Warning conditions.

Sample Syslog Events

Port 1 link up and down
Port Security Limit Control reached but the action is none
IP source guard table is full
IP source guard table reaches the port limitation
IP source guard port limitation changes, should delete entry.
Switch boot up
SNMP authentication failure

For related Alarm information, see the **Alarm** commands.

Command: Configure Loop Protection

Syntax: **config loop-protect**

Description: Configure loop protection. Loops inside a network are costly, as they consume all the resources and reduce network performance. Detecting the loops manually can be cumbersome. Loop Protection can be enabled or disabled on a port and system-wide. If loop protection is enabled, it sends packets to a reserved layer 2 multicast destination address on all the ports on which the feature is enabled. You can disable transmission of the packet on selective ports, even when the loop protection is on. If a packet is received by the switch with a matching multicast destination address, the source MAC in the packet is compared with its own MAC. If the MAC does not match, the packet is forwarded to all ports that are a member of the same VLAN except to the port from which it came in, treating it similar to a data packet. If loop protection is enabled and the source MAC matches its own MAC, the port on which the packet is received will be shutdown, logged, or both actions taken depending upon the action configured. If loop protection is disabled,the packet will be dropped silently.

shutdown-time : The period (in seconds) for which a port will be kept disabled if a loop is detected (and the port action shuts down the port). Valid values are 0 - 604800 seconds (7 days). A value of zero (0) will keep a port disabled (until the next device restart).

transmission-time : The interval between each loop protect PDU sent on each port (1-10 seconds).

Mode: (config)#

Example: Display the various loop protection command functions.

```
(config)# loop ?
    shutdown-time    Loop protection shutdown time interval (0-604800 seconds).
    transmit-time    Loop protection transmit time interval (1-10 seconds).
    <cr>
(config)# loop-protect shutdown-time ?
    <0-604800>    Shutdown time in second
(config)# loop-protect shutdown-time 4 ?
    <cr>
(config)# loop-protect transmit-time ?
    <1-10>    Transmit time in second
(config)# loop-protect transmit-time 1 ?
    <cr>
(config)# loop-protect transmit-time 1
```

Note: STP and Loop Protection may interfere with each other and are not recommended to be enabled on the same physical ports.

Note: If using the S4224 Loop Protection function, enable Loop Protection here, both globally and at the port level, as one of the first overall configuration steps.

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. If you will be using the Loop Protection function, enable Loop Protection here, both globally and at the port level, as one of the first overall configuration steps.

Command: Configure MAC Addr

Syntax: **mac address-table aging**
mac address-table learning
mac address-table static

Description: Configure MAC address aging time and MAC address table entries. Enter a value of **0** to disable MAC aging time.
mac address-table aging-time <v_0_10_to_1000000>
mac address-table learning vlan <vlan_list>
mac address-table static <v_mac_addr> vlan <v_vlan_id> interface (<port_type> [<v_port_type_list>])

Mode: (config)#

Example: Display the available MAC address commands and configure:

```
(config)# mac address-table ?
    aging-time    Mac address aging time
    learning      Mac Learning
    static        Static MAC address
(config)# mac address-table
(config)# mac addr aging-time ?
    <0,10-1000000>    Aging time in seconds, 0 disables aging
(config)# mac addr aging-time 5000 ?
    <cr>
(config)# mac addr aging-time 5000
(config)# mac addr learning ?
    vlan    VLAN
(config)# mac addr learning vlan ?
    <vlan_list>
(config)# mac addr learning vlan 100 ?
    <cr>
(config)# mac addr learning vlan 100
(config)# mac addr static ?
    <mac_addr>    48 bit MAC address: xx:xx:xx:xx:xx:xx
(config)# mac addr static 01:00:00:11:00:00 ?
    vlan    VLAN keyword
(config)# mac addr static 01:00:00:11:00:00 vlan ?
    <vlan_id>    VLAN IDs 1-4095
(config)# mac addr static 01:00:00:11:00:00 vlan 200 ?
    interface    Select an interface to configure
(config)# mac addr static 01:00:00:11:00:00 vlan 200 interface ?
    *                    All switches or All ports
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
(config)# mac addr static 01:00:00:11:00:00 vlan 200 interface * ?
    <port_type_list>    Port list for all port types
    <cr>
(config)# mac addr static 01:00:00:11:00:00 vlan 200 interface *
(config)#
```

The static entries can be configured in the MAC table for forwarding. The static MAC table can contain 64 entries. The MAC table is sorted first by VLAN ID and then by MAC address.

Command: Configure MEP

Syntax: **mep** <uint> [mip] { up | down } domain { port | evc | vlan } [vid <vlan_id>]

Description: Configure MEP (Maintenance Entity End Point) parameters. Flow OAM is implemented as a set of features as per requirements in IEEE802.1ag and ITU-T.Y1731/G.8021. Nodes can be configured as Maintenance End Point (MEP) or Maintenance Intermediate Point (MIP) in an OAM domain to participate in the Flow OAM functionality. Features such as Link Trace, Continuity Check and Alarm Indication Signal are provided in the implementation.

IEEE802.1 ag support is implemented with the features like Link Trace, Loopback and Continuity Check. Message parameters are framed as per the IEEE standard when the Link Trace feature configuration indicates IEEE Link Trace. The ***LTM*** (Link Trace Message) PDU is initiated by MEP. MIPs receive and handle the PDU in a manner that allows the MEP to trace the path to the target MAC address. All intermediate MIPs will forward the packet to the egress port for which the target MAC is learnt and at the same time reply to the MEP with a ***LTR*** (Link Trace Reply). This continues untill the PDU is received by the management point with the target MAC. This entity does not forward the packet but replies to the originator MEP.

The MEP establishes the path by collating all the LTR PDUs.

A **Down MEP** is a MEP residing in a Bridge that receives SOAM PDUs from, and transmits them towards, the direction of the LAN. Note that in the MEF service model, the LAN is a transmission facility in the egress direction, rather than towards the Bridge Relay Entity. Down MEP Restrictions: TBD.

An **Up MEP** is a MEP residing in a Bridge that transmits SOAM PDUs towards, and receives them from, the direction of the Bridge Relay Entity.

A **MIP** (MEG Intermediate Point) is a SOAM point associated with a single MEG level (and a single Maintenance Domain). A MIP can respond to SOAM protocols, but cannot generate requests. MIPs are defined to be located at External Interfaces such as ENNIs (or UNIs). In practice, a MIP can also be used in additional internal operator locations where monitoring is desired.

The default MEG Levels are shown below per MEF 30 (not all MEG levels are required in every application).

Mode: (config)#

Example 1: Display the MEP command options:

```
(config)# mep?
    mep    Maintenance Entity Point
(config)# mep ?
    <1-100>     The MEP instance number.
    os-tlv      Organization-Specific TLV
(config)# mep
```

Example 2: Configure MEPs and show resulting config. Note that “MPLS-TP not supported”.

```
(config)# mep 1 ?
    ais                         Alarm Indication Signal
    aps                         Automatic Protection Switching protocol.
    cc                          Continuity Check.
    ccm-tlv                     The CCM TLV enable/disable
    client                      Transport layer Client.
    dm                          Delay Measurement.
    down                        This MEP is a Down-MEP.
    lb                          Loop Back.
    lck                         Locked Signal.
    level                       The MEG level of the MEP.
    link-state-tracking         Link State Tracking. When LST is enabled in an
                                instance, Local SF or received 'isDown' in CCM
                                Interface Status TLV, will bring down the
                                residence port. Only valid in Up-MEP.
    lm                          Loss Measurement.
    lt                          Link Trace.
    meg-id                      The ITU/IEEE MEG-ID.
    mep-id                      The MEP-ID.
    mip                         This MEP instance is a half-MIP.
    peer-mep-id                 The peer MEP-ID.
    performance-monitoring      Performance monitoring Data Set collection (MEF35).
    syslog                      Enable syslog.
    tst                         Test Signal
    up                          This MEP is a UP-MEP.
    vid                         The MEP VID.
    voe                         MEP is VOE based.
(config)# mep 1 up domain ?
    evc          This MEP is a EVC domain MEP.
    lsp          This MIP is an MPLS-TP LSP domain MIP.
    port         This MEP is a Port domain MEP.
    pw           This MEP is an MPLS-TP Pseudo-Wire domain MEP.
    tp-link      This MEP is an MPLS-TP link domain MEP.
    tunnel-tp    This MEP is an MPLS-TP tunnel domain MEP.
    vlan         This MEP is a VLAN domain MEP.
(config)# mep 1 up domain evc flow 1 level 1 interface GigabitEthernet 1/2
(config)# mep 1 up domain lsp flow 1 level 5 interface 10GigabitEthernet 1/2
(config)# mep 1 up domain port flow 3 level 4 interface GigabitEthernet ½
(config)# mep 2 down domain pw flow 2 level 0
(config)# mep 2 down domain tp-link flow 3 level 2
(config)# mep 3 down domain tunnel-tp flow 2 level 3
(config)# $3 up domain vlan flow 1 level 2 interface 10GigabitEthernet 1/2
(config)#end
# show mep

MEP state is:
  Inst  cLevel  cMeg  cMep  cAis  cLck cLoop cConf  cSsf  aBlk  aTsf  Peer MEP
cLoc  cRdi cPeriod cPrio
     1   False False False False False False False False False False
     3   False False False False False False False False False False
#
```

Note: the MPLS-TP parameters are not currently supported.

Example 3: Configure MEP 1 AIS, APS, CC, Client Domain,

```
(config)# mep 1 ?
    ais                         Alarm Indication Signal
    aps                         Automatic Protection Switching protocol.
    cc                          Continuity Check.
    ccm-tlv                     The CCM TLV enable/disable
    client
    dm                          Delay Measurement.
    down                        This MEP is a Down-MEP.
    lb                          Loop Back.
    lck                         Locked Signal.
    level                       The MEG level of the MEP.
    link-state-tracking         Link State Tracking. When LST is enabled in an
                                instance, Local SF or received 'isDown' in CCM
                                Interface Status TLV, will bring down the
                                residence port. Only valid in Up-MEP.
    lm                          Loss Measurement.
    lt                          Link Trace.
    meg-id                      The ITU/IEEE MEG-ID.
    mep-id                      The MEP-ID.
    mip                         This MEP instance is a half-MIP.
    peer-mep-id                 The peer MEP-ID.
    performance-monitoring      Performance monitoring Data Set collection
                                (MEF35).
    syslog                      Enable syslog.
    tst                         Test Signal
    up                          This MEP is a UP-MEP.
    vid                         The MEP VID.
    voe                         MEP is VOE based.
(config)# mep 1 ais ?
    fr1m        Frame rate is 1 f/min.
    fr1s        Frame rate is 1 f/s.
    protect     The AIS can be used for protection. At the point of state change
                three AIS PDU is transmitted as fast as possible.
    <cr>
(config)# mep 1 ais fr1s ?
    protect     The AIS can be used for protection. At the point of state change
                three AIS PDU is transmitted as fast as possible.
    <cr>
(config)# mep 1 ais fr1s
(config)# mep 1 ais fr1m
(config)# mep 1 ais
(config)# mep 1 ais protect ?
    fr1m    Frame rate is 1 f/min.
    fr1s    Frame rate is 1 f/s.
    <cr>
(config)# mep 1 ais protect
Error: Invalid parameter error returned from MEP
(config)# mep 1 ais protect fr1s
Error: Invalid parameter error returned from MEP

(config)# mep 1 aps ?
    <Prio : 0-7>    Priority in case of tagged OAM. In the EVC domain this is
                    the COS-ID.
(config)# mep 1 aps 2 ?
    laps      Linear Automatic Protection Switching protocol.
    multi     OAM PDU is transmitted with multicast MAC. Must me 'multi' in case
              of RAPS.
    raps      Ring Automatic Protection Switching protocol.
    uni       OAM PDU is transmitted with unicast MAC. The MAC is taken from
              peer MEP MAC database. Only possible in case of LAPS.
```

```
(config)# mep 1 aps 2 raps ?
    octet    Then last OCTET in the multivast MAC. Only possible in case of
             RAPS.
    <cr>
(config)# mep 1 aps 2 raps
(config)# mep 1 cc ?
    <Prio : 0-7>    Priority in case of tagged OAM. In the EVC domain this is
                    the COS-ID.
(config)# mep 1 cc 3 ?
    fr100s    Frame rate is 100 f/s.
    fr10s     Frame rate is 10 f/s.
    fr1m      Frame rate is 1 f/min.
    fr1s      Frame rate is 1 f/s.
    fr300s    Frame rate is 300 f/s.
    fr6h      Frame rate is 6 f/hour.
    fr6m      Frame rate is 6 f/min.
    <cr>
(config)# mep 1 cc 3 fr1s ?
    <cr>
(config)# mep 1 cc 3 fr1s
Error: Invalid number of peer's for this configuration
(config)# mep 2 client ?
    domain    Domain.
(config)# mep 2 client domain ?
    evc     EVC client flow.
    lsp     MPLS-TP LSP client flow.
    vlan    VLAN client flow.
(config)# mep 2 client domain evc ?
    flow
    <cr>
(config)# mep 2 client domain evc flow ?
    <uint>
(config)# mep 2 client domain evc flow 2 ?
    level    The MEG level on the client layer.
(config)# mep 2 client domain evc flow 2 level ?
    <0-7>    The MEG level value.
(config)# mep 2 client domain evc flow 2 level 1 ?
    ais-prio    AIS injection priority.
    lck-prio    LCK injection priority.
    <cr>
(config)# mep 2 client domain evc flow 2 level 1 ais-prio ?
    <0-7>          AIS injection priority value.
    ais-highest    Request the highest possible AIS priority.
    lck-prio       LCK injection priority.
    <cr>
(config)# mep 2 client domain evc flow 2 level 1 ais-prio 3 ?
    lck-prio    LCK injection priority.
    <cr>
(config)# mep 2 client domain evc flow 2 level 1 ais-prio 3 lck-prio ?
    <0-7>          LCK injection priority value.
    lck-highest    Request the highest possible LCK priority.
    <cr>
(config)# mep 2 client domain evc flow 2 level 1 ais-prio 3 lck-prio
(config)# mep 1 down domain vlan ?
    flow    The flow instance that the MEP is related to.
    vid     In case the MEP is a port Up-MEP or a EVC customer MIP the VID must
            be given.
(config)# mep 1 down domain vlan vid 1 ?
    flow    The flow instance that the MEP is related to.
(config)# mep 1 down domain vlan vid 1 flow ?
    <Flow : uint>    The flow instance number when not in the port domain.
```

```
(config)# mep 1 down domain vlan vid 1 flow 1 ?
    level    The MEG level of the MEP.
(config)# mep 1 down domain vlan vid 1 flow 1 level ?
    <Level : 0-7>    The MEG level value.
(config)# mep 1 down domain vlan vid 1 flow 1 level 5 ?
    interface    The recidence port of the MEP.
(config)# mep 1 down domain vlan vid 1 flow 1 level 5 interface ?
    GigabitEthernet       1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
(config)# mep 1 down domain vlan vid 1 flow 1 level 5 interface g ?
    PORT_ID    Port ID in 1/1-6
(config)# mep 1 down domain vlan vid 1 flow 1 level 5 interface g 1/1 ?
    <cr>
(config)# mep 1 down domain vlan vid 1 flow 1 level 5 interface g 1/1
MEP instance is already created - must be deleted first
(config)#
```

Example 4: Configure MEP 1 LoopBack (LB) parameters.

```
(config)# mep 1 lb ?
    <0-7>    Priority in case of tagged OAM. In the MPLS and EVC domain this is the COS-ID.
(config)# mep 1 lb 3 ?
    count    The number of LBM PDUs to send in one loop test. The value 0
             indicate infinite transmission (test behaviour). This is HW based
             LBM/LBR and Requires VOE.
    dei      Drop Eligible Indicator in case of tagged OAM.
    mpls     Specify optional values for loopback initiated from an MPLS-TP MEP.
    multi    OAM PDU is transmitted with multicast MAC. Not used for MPLS-TP.
    uni      OAM PDU is transmitted with unicast MAC. The MAC is taken from
             peer MEP MAC database. Not used for MPLS-TP.
(config)# mep 1 lb 3 multi ?
    count    The number of LBM PDU to send in one loop test. The value 0
             indicate infinite transmission (test behaviour). This is HW based
             LBM/LBR and Requires VOE.
    dei      Drop Eligible Indicator in case of tagged OAM.
(config)# mep 1 lb 3 multi dei ?
    count    The number of LBM PDU to send in one loop test. The value 0
             indicate infinite transmission (test behaviour). This is HW based
             LBM/LBR and Requires VOE.
(config)# mep 1 lb 3 multi dei c ?
    <Count : uint>    Number of LBM PDU to send value.
(config)# mep 1 lb 3 multi dei count ?
    <Count : uint>    Number of LBM PDU to send value.
(config)# mep 1 lb 3 multi dei count 5 ?
    size    The number of bytes in the LBM PDU Data Pattern TLV
(config)# mep 1 lb 3 multi dei count 5 size ?
    <uint>    The LBM frame size. This is entered as the wanted size (in bytes)
              of a un-tagged frame containing LBM OAM PDU - including CRC (four
              bytes). Example when 'Size' = 64 => Un-tagged frame size =
              DMAC(6) + SMAC(6) + TYPE(2) + LBM PDU LENGTH(46) + CRC(4) = 64 by
(config)# mep 1 lb 3 multi dei count 5 size 32 ?
    interval    The number of bytes in the LBM PDU Data Pattern TLV
(config)# mep 1 lb 3 multi dei count 5 size 32
(config)# mep 1 lb 3 multi dei count 5 size 32 interval ?
    <uint>    The interval between transmitting LBM PDU. in case 'count' != 0
              this is in 10ms and max is 100. In case 'count' == 0 this is in
              1us and max is 10.000.
(config)# mep 1 lb 3 multi dei count 5 size 32 interval 5 ?
    <cr>
(config)# mep 1 lb 3 multi dei count 5 size 32 interval 5
Error: Invalid parameter error returned from MEP
(config)# mep 1 lck ?
```

```
    fr1m    Frame rate is 1 f/min.
    fr1s    Frame rate is 1 f/s.
    <cr>
(config)#
```

Example 5: Configure MEP 1 LM (Loss Measurement) parameters.

```
(config)# mep 1 lck ?
    fr1m    Frame rate is 1 f/min.
    fr1s    Frame rate is 1 f/s.
    <cr>
(config)# mep 1 level ?
    <Level : 0-7>    The MEG level value.
(config)# mep 1 level 4 ?
    <cr>
(config)# mep 1 level 4
Error: Invalid number of peer's for this configuration
(config)# mep 1 lm ?
    <0-7>            Priority in case of tagged OAM. In the MPLS and EVC domain
                     this is the COS-ID.
    flow-counting    Loss Measurement is counting service frames per flow - all
                     priority in one.
    oam-counting     Loss Measurement is counting OAM frames either as Y1731 or
                     all
(config)# mep 1 lm 0 ?
    dual      Dual ended LM is based on CCM PDU.
    flr       The Frame Loss Ratio interval.
    fr10s     Frame rate is 10 f/s.
    fr1m      Frame rate is 1 f/min.
    fr1s      Frame rate is 1 f/s.
    fr6h      Frame rate is 6 f/hour.
    fr6m      Frame rate is 6 f/min.
    multi     OAM PDU is transmitted with multicast MAC.
    single    Single ended LM is based on LMM/LMR PDU.
    uni       OAM PDU is transmitted with unicast MAC. The MAC is taken from
              peer MEP MAC database. In case of LM there is only one peer MEP.
    <cr>
(config)# mep 1 lm 0 single ?
    flr      The Frame Loss Ratio interval.
    fr10s    Frame rate is 10 f/s.
    fr1m     Frame rate is 1 f/min.
    fr1s     Frame rate is 1 f/s.
    fr6h     Frame rate is 6 f/hour.
    fr6m     Frame rate is 6 f/min.
    multi    OAM PDU is transmitted with multicast MAC.
    uni      OAM PDU is transmitted with unicast MAC. The MAC is taken from
             peer MEP MAC database. In case of LM there is only one peer MEP.
    <cr>

(config)# mep 1 lm 0 single flr ?
    <Flr : uint>    The Frame Loss Ratio interval value.
(config)# mep 1 lm 0 single flr 5 ?
    fr10s    Frame rate is 10 f/s.
    fr1m     Frame rate is 1 f/min.
    fr1s     Frame rate is 1 f/s.
    fr6h     Frame rate is 6 f/hour.
    fr6m     Frame rate is 6 f/min.
    multi    OAM PDU is transmitted with multicast MAC.
    uni      OAM PDU is transmitted with unicast MAC. The MAC is taken from
             peer MEP MAC database. In case of LM there is only one peer MEP.
    <cr>
```

```
(config)# mep 1 lm 0 single flr 5 fr1m
Error: Invalid parameter error returned from MEP
(config)# mep 1 lt ?
    <Prio : 0-7>    Priority in case of tagged OAM. In the EVC domain this is the COS-ID.
```

Example 6: Configure MEP 1 LT (Link Trace) parameters.

```
(config)# mep 1 lt 4 ?
    mac       Link Trace target unicast MAC to be used in case of LT against
              MIP.
    mep-id    Peer MEP-ID for Link Trace target unicast MAC. The MAC is taken
              from peer MEP MAC database.
(config)# mep 1 lt 4 mep-id ?
    <Mepid : uint>    Peer MEP-ID value.
(config)# mep 1 lt 4 mep-id 1 ?
    ttl    Time To Live.
(config)# mep 1 lt 4 mep-id 1 ttl ?
    <Ttl : uint>    Time To Live value.
(config)# mep 1 lt 4 mep-id 1 ttl 3 ?
    <cr>
(config)# mep 1 lt 4 mep-id 1 ttl 3
Error: Invalid number of peer's for this configuration
```

Example 7: Configure MEP 1 MEG ID and MEP ID parameters.

```
(config)# mep 1 meg-id ?
    <Megid : word>    The MEG-ID string. This is either the ITU MEG-ID or the
                      IEEE Short MA, depending on the selected MEG-ID format.
                      The ITU max. is 13 characters. The ITU-CC max. is 15
                      characters. The IEEE max. is 16 characters.
(config)# mep 1 meg-id ItuMegId100 ?
    ieee      The MEG-ID (Short MA Name) has IEEE Character String format. The
              meg-id max. is 16 characters.
    itu       The MEG-ID has ITU format (ICC - UMC). The meg-id max. is 13
              characters.
    itu-cc    The MEG-ID has ITU Country Code format (CC - ICC - UMC). The
              meg-id max. is 15 characters
(config)# mep 1 meg-id ItuMegId100 itu ?
    <cr>
(config)# mep 1 meg-id ItuMegId100 itu
Error: Invalid number of peer's for this configuration
(config)# mep 1 mep-id ?
    <Mepid : uint>    The MEP-ID value.
(config)# mep 1 mep-id 1 ?
    <cr>
(config)# mep 1 mep-id 1
```

Example 8: Configure MEP MIP parameters.

```
(config)# mep 1 mip ?
    down    This MEP is a Down-MEP.
    up      This MEP is a UP-MEP.
(config)# mep 1 mip down ?
    domain    The domain of the MEP.
(config)# mep 1 mip down domain ?
    evc           This MEP is a EVC domain MEP.
    lsp           This MIP is an MPLS-TP LSP domain MIP.
    port          This MEP is a Port domain MEP.
    pw            This MEP is an MPLS-TP Pseudo-Wire domain MEP.
    tp-link       This MEP is an MPLS-TP link domain MEP.
    tunnel-tp     This MEP is an MPLS-TP tunnel domain MEP.
    vlan          This MEP is a VLAN domain MEP.
(config)# mep 1 mip down domain vlan ?
    flow    The flow instance that the MEP is related to.
    vid     In case the MEP is a port Up-MEP or a EVC customer MIP the VID must
            be given.
(config)# mep 1 mip down domain vlan vid ?
    <Vid : vlan_id>    The port Domain MEP VID. This is required for a Port
                       Up-MEP.
(config)# mep 1 mip down domain vlan vid 1 ?
    flow    The flow instance that the MEP is related to.
(config)# mep 1 mip down domain vlan vid 1 flow ?
    <Flow : uint>    The flow instance number when not in the port domain.
(config)# mep 1 mip down domain vlan vid 1 flow 2 ?
    level    The MEG level of the MEP.
(config)# mep 1 mip down domain vlan vid 1 flow 2 level ?
    <Level : 0-7>    The MEG level value.
(config)# mep 1 mip down domain vlan vid 1 flow 2 level 1 ?
    interface    The recidence port of the MEP.
(config)# mep 1 mip down domain vlan vid 1 flow 2 level 1 interface ?
    GigabitEthernet       1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
(config)# mep 1 mip down domain vlan vid 1 flow 2 level 1 interface g ?
    PORT_ID    Port ID in 1/1-6
(config)# mep 1 mip down domain vlan vid 1 flow 2 level 1 interface g 1/1 ?
    <cr>
(config)# mep 1 mip down domain vlan vid 1 flow 2 level 1 interface g 1/1
MEP instance is already created - must be deleted first
(config)#
```

Example 9: Configure Peer MEP parameters.

```
(config)# mep 2 peer-mep-id ?
    <Mepid : uint>    The peer MEP-ID value.
(config)# mep 2 peer-mep-id 2 ?
    mac     The peer MAC. this will be overwritten by any learned MAC - through CCM reception.
    <cr>
(config)# mep 2 peer-mep-id 2
This MEP is not enabled
(config)# mep 1 peer-mep-id 2
```

Example 10: Configure MEP 1 PM (Performance Monitoring) parameters.

```
(config)# mep 1 performance-monitoring ?
    <cr>
(config)# mep 1 performance-monitoring
(config)# mep 1 performance-monitoring ?
    <cr>
(config)# mep 1 performance-monitoring?
    performance-monitoring    Performance monitoring Data Set collection (MEF35).
    <cr>
(config)# mep 1 performance-monitoring?
mep <inst> performance-monitoring
(config)# mep 1 performance-monitoring
(config)#
```

Example 11: Configure MEP TST (Test Signal) parameters.

```
(config)# mep 1 tst ?
    <0-7>    Priority in case of tagged OAM. In the MPLS and EVC domain this is the COS-ID.
    rx       Receive Test Signal.
    tx       Transmit Test Signal.
(config)# mep 1 tst 1 ?
    dei       Drop Eligible Indicator in case of tagged OAM.
    mep-id    Peer MEP-ID for unicast TST. The MAC is taken from peer MEP MAC
              database.
(config)# mep 1 tst 1 mep-id ?
    <Mepid : uint>    Peer MEP-ID value.
(config)# mep 1 tst 1 mep-id 1 ?
    all-one     Test pattern is set to all one.
    all-zero    Test pattern is set to all zero.
    one-zero    Test pattern is set to 10101010.
    rate        The TST frame transmission bit rate - in Megabits per second.
                Limit on Serval is 1Gbps. This is the bit rate of a standard frame without any
                encapsulation. If 1 Mbps rate is selected in a EVC MEP, the added tag will
               give a hi.
    sequence    Enable sequence number in TST PDU.
(config)# mep 1 tst 1 mep-id 1 all-one ?
    rate        The TST frame transmission bit rate - in Mega bits pr. second.
                Limit on Caracal is 400 Mbps. Limit on Serval is 1Gbps. This is
                the bit rate of a standard frame without any encapsulation. If
                1 Mbps rate is selected in a EVC MEP, the added tag will give a
                hi
    sequence    Enable sequence number in TST PDU.
(config)# mep 1 tst 1 mep-id 1 all-one rate 100 ?
    size    The TST frame size. This is entered as the wanted size (in bytes)
            of a un-tagged frame containing TST OAM PDU - including CRC (four
            bytes). Example when 'Size' = 64 => Un-tagged frame size = DMAC(6)
            + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 by
(config)# mep 1 tst 1 mep-id 1 all-one rate 100 size ?
    <Size : uint>    Frame size value.
(config)# mep 1 tst 1 mep-id 1 all-one rate 100 size 100 ?
    <cr>
(config)# mep 1 tst 1 mep-id 1 all-one rate 100 size 100
```

Example 12: Configure MEP 1 as a MIP.

```
(config)# mep 1 up ?
    domain    The domain of the MEP.
(config)#
(config)# mep 1 up?
    up    This MEP is a UP-MEP.
(config)# mep 1 up?
    up    This MEP is a UP-MEP.
(config)# mep 1 up?
mep <inst> [ mip ] { up | down } domain { port | evc | vlan | tp-link | tunnel-tp | pw | lsp }
[ vid <vid> ] [ flow <flow> ] level <level> [ interface <port_type> <port> ]
(config)# mep 1 up domain ?
    evc           This MEP is a EVC domain MEP.
    lsp           This MIP is an MPLS-TP LSP domain MIP.
    port          This MEP is a Port domain MEP.
    pw            This MEP is an MPLS-TP Pseudo-Wire domain MEP.
    tp-link       This MEP is an MPLS-TP link domain MEP.
    tunnel-tp     This MEP is an MPLS-TP tunnel domain MEP.
    vlan          This MEP is a VLAN domain MEP.
(config)# mep 1 up domain vlan ?
    flow      In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
              Pseudo-Wire domain MEP, the flow instance that the MEP is related
              to must be given.
    level     The MEG level of the MEP.
    vid       In case the MEP is a Port domain Up-MEP or a EVC domain customer
              MIP (on the UNI), the VID must be given.
(config)# mep 1 up domain vlan flow 1 ?
    level     The MEG level of the MEP.
    vid       In case the MEP is a Port domain Up-MEP or a EVC domain customer
              MIP (on the UNI), the VID must be given.
(config)# mep 1 up domain vlan flow 1 level ?
    <Level : 0-7>    The MEG level value.
(config)# mep 1 up domain vlan flow 1 level 2 ?
    interface    The recidence port of the MEP.
(config)# mep 1 up domain vlan flow 1 level 2 interface ?
    GigabitEthernet       1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
(config)# mep 1 up domain vlan flow 1 level 2 interface 2 ?
    PORT_ID    Port ID in 1/1-2
(config)# mep 1 up domain vlan flow 1 level 2 interface 2 ?
    PORT_ID    Port ID in 1/1-2
(config)# mep 1 up domain vlan flow 1 level 2 interface 2 1/1
MEP instance is already created - must be deleted first
(config)#
```

Example 13: Configure MEP 1 VID (VLAN ID) parameters.

```
(config)# mep 1 vid ?
    <Vid : vlan_id>    The MEP VID value.
(config)# mep 1 vid 1 ?
    <cr>
(config)# mep 1 vid 1
(config)# mep 1 vid 1 ?
    <cr>
(config)# mep 1 vid 1
(config)# mep 1 vid 2
```

Note: the MPLS-TP parameters are not currently supported.

Messages

% No such port: 10GigabitEthernet 1/3
Error: No VOE available
Error: MPLS-TP: Invalid MPLS-TP link interface number
Error: This MIP is not supported
Error: VLAN is not created for this VID
MPLS-TP not supported
MPLS-TP can not have 'interface'
MPLS-TP tunnel can only have down MIP/MEP
This MEP is not enabled

MEP Config Parameters Summary

(config)# **mep??**
mep <inst> [mip] { up | down } domain { port | evc | vlan | tp-link | tunnel-tp | pw | lsp } [vid <vid>] [flow <flow>] level <level> [interface <port_type> <port>]
mep <inst> ais [fr1s | fr1m] [protect]
mep <inst> aps <prio> [multi | uni] { laps | { raps [octet <octet>] } }
mep <inst> cc <prio> [fr300s | fr100s | fr10s | fr1s | fr6m | fr1m | fr6h]
mep <inst> ccm-tlv
mep <inst> client domain { evc | vlan | lsp } flow <cflow> [level <level>] [ais-prio [<aisprio> | ais-highest]] [lck-prio [<lckprio> | lck-highest]]mep <inst> dm <prio> [multi | { uni mep-id <mepid> }] [single | dual] [rdtrp | flow] interval <interval> last-n <lastn>
mep <inst> dm bin fd <num_fd_var>
mep <inst> dm bin ifdv <num_ifdv_var>
mep <inst> dm bin threshold <threshold_var>
mep <inst> dm ns
mep <inst> dm overflow-reset
mep <inst> dm proprietary
mep <inst> dm syncronized
mep <inst> lb <prio> [dei] [multi | { uni { { mep-id <mepid> } | { mac <mac>} } } | mpls ttl <mpls_ttl>] count <count> size <size> interval <interval>
mep <inst> lck [fr1s | fr1m]
mep <inst> level <level>
mep <inst> link-state-tracking
mep <inst> lm <prio> [multi | uni] [single | dual] [fr10s | fr1s | fr6m | fr1m | fr6h] [flr <flr>]
mep <inst> lm flow-counting
mep <inst> lm oam-counting { [y1731 | all] }
mep <inst> lt <prio> { { mep-id <mepid> } | { mac <mac> } } ttl <ttl>
mep <inst> meg-id <megid> { itu | itu-cc | { ieee [name <name>] } }
mep <inst> mep-id <mepid>
mep <inst> peer-mep-id <mepid> [mac <mac>]
mep <inst> performance-monitoring
mep <inst> syslog
mep <inst> tst <prio> [dei] mep-id <mepid> [sequence] [all-zero | all-one | one-zero] rate <rate> size <size>
mep <inst> tst rx
mep <inst> tst tx
mep <inst> vid <vid>
mep os-tlv oui <oui> sub-type <subtype> value <value>
(config)# mep

Note: the MPLS-TP parameters are not currently supported.

Command: Configure MEP AIS

Syntax: **mep** <inst> **ais** [fr1s | fr1m] [protect]

Description: Configure the enabled MEP Alarm Indication Signal in terms of frame rate and protection. AIS provides indication of service interruption upstream, and is recommended for point to point services. AIS is signaled by peer MEPs away from each other to indicate a network fault (not created by MIPs).

AIS gets sent at the next available MEG level, and is propagated at higher MEG level at MEPs.

AIS messages must be sent immediately and then at regular intervals (the default is 1frame/second).

The AIS default CoS ID should correspond to the CoS which yields the lowest frame loss. AIS is declared immediately on receipt of an AIS PDU, and cleared after not receiving an AIS PDU for 3.5 times the transmission interval. “ETH-AIS” is the AIS Message.
AIS is transmitted by a MEP during Signal Fail conditions. It can be used for suppression of alarm on client layer or for protection on client layer.

Mode: (config)#

Example: Display the various command functions:

```
(config)# mep 1 ais ?
    fr1m       Frame rate is 1 frame/minute.
    fr1s       Frame rate is 1 frame/second (default).
    protect    The AIS can be used for protection. At the point of state change three
               AIS PDU is transmitted as fast as possible.
    <cr>
```

Command: Configure MEP APS

Syntax: **mep** <inst> **aps** <prio> [multi | uni] { laps | { raps [octet <octet>] } }

Description: Configure the enabled MEP's Automatic Protection Switching parameters.

<**0**-**7**> Priority in case of tagged OAM. In the MPLS and EVC domain this is the COS-ID.
laps Linear Automatic Protection Switching protocol.
multi OAM PDU is transmitted with multicast MAC. Must be 'multi' in case of RAPS.
raps Ring Automatic Protection Switching protocol.
uni OAM PDU is transmitted with unicast MAC. The MAC is taken from peer MEP MAC database. Only possible in case of LAPS.
octet Then last OCTET in the multivast MAC. Only possible in case of RAPS.

Mode: (config)#

Example: Configure an enabled MEP's Automatic Protection Switching parameters:

```
(config)# mep 1 aps ?
    <Prio : 0-7>    Priority in case of tagged OAM. In the EVC domain this is the COS-ID.
(config)# mep 1 aps 2 ?
    laps     Linear Automatic Protection Switching protocol.
    multi    OAM PDU is transmitted with multicast MAC. Must me 'multi' in case of RAPS.
    raps     Ring Automatic Protection Switching protocol.
    uni      OAM PDU is transmitted with unicast MAC. The MAC is taken from
             peer MEP MAC database. Only possible in case of LAPS.
(config)# mep 1 aps 2 ?
    laps     Linear Automatic Protection Switching protocol.
    multi    OAM PDU is transmitted with multicast MAC. Must me 'multi' in case
             of RAPS.
    raps     Ring Automatic Protection Switching protocol.
    uni      OAM PDU is transmitted with unicast MAC. The MAC is taken from
             peer MEP MAC database. Only possible in case of LAPS.
(config)# mep 1 aps 2 laps ?
    <cr>
(config)# mep 1 aps 2 multi ?
    laps    Linear Automatic Protection Switching protocol.
    raps    Ring Automatic Protection Switching protocol.
(config)# mep 1 aps 2 multi laps ?
    <cr>
(config)# mep 1 aps 2 multi raps ?
    octet    Then last OCTET in the multivast MAC. Only possible in case of
             RAPS.
    <cr>
(config)# mep 1 aps 2 raps ?
    octet    Then last OCTET in the multivast MAC. Only possible in case of
             RAPS.
    <cr>
(config)# mep 1 aps 2 uni ?
    laps    Linear Automatic Protection Switching protocol.
    raps    Ring Automatic Protection Switching protocol.
(config)# mep 1 aps 2 uni laps ?
    <cr>
(config)# mep 1 aps 2 uni raps ?
    octet    Then last OCTET in the multivast MAC. Only possible in case of
             RAPS.
    <cr>
(config)# mep 1 aps 2 uni raps
(config)#
```

Command: Configure MEP CC

Syntax: **mep** <inst> **cc** <prio> [fr300s | fr100s | fr10s | fr1s | fr6m | fr1m | fr6h]

Description: Configure the enabled MEP Continuity (Connectivity) Check (CC) parameters.
Connectivity Check Messages (CCMs) verify basic service connectivity and health.CCM transmission is enabled by default on the UNI MEG and the ENNI MEG. CCM transmission is disabled by default on the Subscriber, Test, EVC, SP and Operator MEGs. A MEP supports the CCM frame transmission periods of 1 and 10 seconds (1 second default for UNI/ENNI MEG; other MEG level defaults are 10 seconds).
When three consecutive CCM messages are lost, connectivity failure is declared. When a MEP detects a CCM fault, the RDI bit is set in the CCM message in the opposite direction.
Continuity Check is used for detecting loss of continuity between a MEP and its peer MEP(s).
A CC can also detect unintended connection to other MEG (Maintenance Groups), unintended connection to peer MEP, unexpected period, etc.

Mode: (config)#

Example: Configure the enabled MEP Continuity (Connectivity) Check (CC) parameters.

```
(config)# mep 1 cc ?
    <Prio : 0-7>    Priority in case of tagged OAM. In the EVC domain this is the COS-ID.
(config)# mep 1 cc 4 ?
    fr100s    Frame rate is 100 f/s.
    fr10s     Frame rate is 10 f/s.
    fr1m      Frame rate is 1 f/min.
    fr1s      Frame rate is 1 f/s.
    fr300s    Frame rate is 300 f/s.
    fr6h      Frame rate is 6 f/hour.
    fr6m      Frame rate is 6 f/min.
    <cr>
(config)# mep 1 cc 4 fr1s ?
    <cr>
(config)# mep 1 cc 4 fr1s
```

Command: Configure MEP CCM-TLV

Syntax: **mep 1 ccm-tlv**

Description: Enable/disable the MEP CCM TLV. CCM (Continuity Check Message) is an OAM frame transmitted from a MEP to it's peer MEP and used to implement CC functionality.
TLV (Type Length Value) involves a LLDP frame that can contain multiple pieces of information. Each of these pieces of information is known as a TLV.

Mode: (config)#

Example: Enable or disable the MEP CCM/TLV:

```
(config)# mep 1 ccm-tlv?
    ccm-tlv    The CCM TLV enable/disable
    <cr>
(config)# mep 1 ccm-tlv
(config)#
```

Command: Configure MEP Transport Layer Client Domain

Syntax: **mep** <inst> **client domain** { evc | vlan }
Description: Configure the enabled MEP client domain parameters.
Evc: This is a MEP in the EVC Domain. 'Flow Instance' is a EVC. The EVC must exist.
Vlan: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. The VLAN must exist.
Mode: (config)#
Example: Configure the MEP client domain and display the resulting config:

```
(config)# mep 1 client domain ?
    evc     EVC client flow.
    lsp     MPLS-TP LSP client flow.
    vlan    VLAN client flow.
(config)# mep 1 client domain evc ?
    flow
    <cr>
(config)# mep 1 client domain evc flow ?
    <uint>
(config)# mep 1 client domain evc flow 1 ?
    level    The MEG level on the client layer.
(config)# mep 1 client domain evc flow 1 level ?
    <0-7>    The MEG level value.
(config)# mep 1 client domain evc flow 1 level 2 ?
    ais-prio    AIS injection priority.
    lck-prio    LCK injection priority.
    <cr>
(config)# mep 1 client domain evc flow 1 level 2
(config)# mep 1 client domain lsp ?
    flow
    <cr>
(config)# mep 1 client domain lsp flow ?
    <uint>
(config)# mep 1 client domain lsp flow 2 ?
    level    The MEG level on the client layer.
(config)# mep 1 client domain lsp flow 2 level ?
    <0-7>    The MEG level value.
(config)# mep 1 client domain lsp flow 2 level 2 ?
    ais-prio    AIS injection priority.
    lck-prio    LCK injection priority.
    <cr>
(config)# mep 1 client domain lsp flow 2 level 2 ais-prio ?
    <0-7>          AIS injection priority value.
    ais-highest    Request the highest possible AIS priority.
    lck-prio       LCK injection priority.
    <cr>
(config)# mep 1 client domain lsp flow 2 level 2 ais-prio
Error: Invalid parameter error returned from MEP
(config)# mep 1 client domain vlan ?
    flow
    <cr>
(config)# mep 1 client domain vlan flow ?
    <uint>
(config)# mep 1 client domain vlan flow 3 ?
    level    The MEG level on the client layer.
(config)# mep 1 client domain vlan flow 3 level ?
    <0-7>    The MEG level value.
(config)# mep 1 client domain vlan flow 3 level 2 ?
    ais-prio    AIS injection priority.
    lck-prio    LCK injection priority.
    <cr>
```

```
(config)# mep 1 client domain vlan flow 3 level 2 lck-prio ?
    <0-7>          LCK injection priority value.
    ais-prio       AIS injection priority.
    lck-highest    Request the highest possible LCK priority.
    <cr>
(config)# mep 1 client domain vlan flow 3 level 2 lck-prio 2 ?
    ais-prio    AIS injection priority.
    <cr>
(config)# mep 1 client domain vlan flow 3 level 2 lck-prio 2
Error: Invalid parameter error returned from MEP
 (config)# do show mep client detail

MEP CLIENT Configuration is:
     Inst     Domain     Client     Flows     AIS Prio     LCK Prio     Level
        1       Port        Evc         1      Highest      Highest         2
        3       Vlan

(config)#
```

Command: Configure MEP DM (Delay Measurement)

Syntax: **mep** <inst> **dm** <prio> [multi | { uni mep-id <mepid> }] [single | dual] [rdtrp | flow] **interval** <interval> last-n <lastn>

Description: Delay Measurement is done between MEPs only. There can be many MEPs in the group, but DM is done between two MEPs only – this is a flow point to multi-point function. Both the one-way and the two-way delay + delay variation can be calculated based on the exchanged information between the MEPs.

Configure the enabled MEP Delay Measurement, where:

dual Delay Measurement based on 1DM PDU transmission.
flow The two way delay is calculated as round trip symmetrical flow delay. The far end residence time is subtracted.
interval Interval between PDU transmissions in 10ms increments. The min. value is 10.
multi OAM PDU is transmitted with multicast MAC.
rdtrp The two way delay is calculated as round trip delay. The far end residence time is not subtracted.
single Delay Measurement based on DMM/DMR PDU.
uni OAM PDU is transmitted with unicast MAC. The MAC is taken from the peer MEP MAC database.

Mode: (config)#

Example: Display the various DM command functions:

```
(config)# mep 1 dm ?
    <0-7>              Priority in case of tagged OAM. In the MPLS and EVC
                       domain this is the COS-ID.
    bin                Delay Measurement Binning.
    ns                 Nano Seconds
    overflow-reset     Reset all Delay Measurement results on total delay counter overflow.
    proprietary        Proprietary Delay Measurement.
    syncronized        Near enad and far end is real time synchronized.
(config)# mep 1 dm 1 ?
    dual         Delay Measurement based on 1DM PDU transmission.
    flow         The two way delay is calculated as round trip symmetrical flow
                 delay. The far end residence time is subtracted.
    interval     Interval between PDU transmission in 10ms. Min value is 10.
    multi        OAM PDU is transmitted with multicast MAC.
    rdtrp        The two way delay is calculated as round trip delay. The far
                 end residence time is not subtracted.
    single       Delay Measurement based on DMM/DMR PDU.
    uni          OAM PDU is transmitted with unicast MAC. The MAC is taken from
                 peer MEP MAC database.
(config)# mep 1 dm bin ?
    fd            the number of FD Measurement Bins.
    ifdv          the number of IFDV Measurement Bins.
    threshold     the threshold for each Delay Measurement Binning.
(config)# mep 1 dm ns ?
    <cr>
(config)# mep 1 dm overflow-reset ?
    <cr>
(config)# mep 1 dm proprietary ?
    <cr>
(config)# mep 1 dm syncronized ?
    <cr>
(config)# mep 1 dm syncronized
```

Example: Display the various DM command parameters:

```
(config)# mep 1 dm?
    dm    Delay Measurement.
(config)# mep 1 dm ?
    <0-7>             Priority in case of tagged OAM. In the MPLS and EVC
                      domain this is the COS-ID.
    bin               Delay Measurement Binning.
    ns                Nano Seconds
    overflow-reset    Reset all Delay Measurement results on total delay
                      counter overflow.
    proprietary       Proprietary Delay Measurement.
    syncronized       Near enad and far end is real time synchronized.
(config)# mep 1 dm 1 ?
    dual        Delay Measurement based on 1DM PDU transmission.
    flow        The two way delay is calculated as round trip symmetrical flow
                delay. The far end residence time is subtracted.
    interval    Interval between PDU transmission in 10ms. Min value is 10.
    multi       OAM PDU is transmitted with multicast MAC.
    rdtrp       The two way delay is calculated as round trip delay. The far
                end residence time is not subtracted.
    single      Delay Measurement based on DMM/DMR PDU.
    uni         OAM PDU is transmitted with unicast MAC. The MAC is taken from
                peer MEP MAC database.
(config)# mep 1 dm ?
    <0-7>             Priority in case of tagged OAM. In the MPLS and EVC
                      domain this is the COS-ID.
    bin               Delay Measurement Binning.
    ns                Nano Seconds
    overflow-reset    Reset all Delay Measurement results on total delay
                      counter overflow.
    proprietary       Proprietary Delay Measurement.
    syncronized       Near enad and far end is real time synchronized.
(config)# mep 1 dm bin ?
    fd           the number of FD Measurement Bins.
    ifdv         the number of IFDV Measurement Bins.
    threshold    the threshold for each Delay Measurement Binning.
(config)# mep 1 dm ns ?
    <cr>
(config)# mep 1 dm overflow-reset ?
    <cr>
(config)# mep 1 dm proprietary ?
    <cr>
(config)# mep 1 dm syncronized ?
    <cr>
(config)# mep 1 dm syncronized
(config)# mep 1 dm 1 ?
    dual        Delay Measurement based on 1DM PDU transmission.
    flow        The two way delay is calculated as round trip symmetrical flow
                delay. The far end residence time is subtracted.
    interval    Interval between PDU transmission in 10ms. Min value is 10.
    multi       OAM PDU is transmitted with multicast MAC.
    rdtrp       The two way delay is calculated as round trip delay. The far
                end residence time is not subtracted.
    single      Delay Measurement based on DMM/DMR PDU.
    uni         OAM PDU is transmitted with unicast MAC. The MAC is taken from
                peer MEP MAC database.
(config)# mep 1 dm 1 dual ?
    flow        The two way delay is calculated as round trip symmetrical flow
                delay. The far end residence time is subtracted.
    interval    Interval between PDU transmission in 10ms. Min value is 10.
    multi       OAM PDU is transmitted with multicast MAC.
```

```
    rdtrp       The two way delay is calculated as round trip delay. The far
                end residence time is not subtracted.
    uni         OAM PDU is transmitted with unicast MAC. The MAC is taken from
                peer MEP MAC database.
(config)# mep 1 dm 1 dual flow ?
    interval    Interval between PDU transmission in 10ms. Min value is 10.
    multi       OAM PDU is transmitted with multicast MAC.
    uni         OAM PDU is transmitted with unicast MAC. The MAC is taken from
                peer MEP MAC database.
(config)# mep 1 dm 1 dual flow interval ?
    <uint>    Interval value.
(config)# mep 1 dm 1 dual flow interval 1 ?
    last-n    The last N dalays used for average last N calculation. Min value
              is 10.
(config)# mep 1 dm 1 dual flow interval 1 ?
mep <inst> dm <prio> [ multi | { uni mep-id <mepid> } ] [ single | dual ] [ rdtr
p | flow ] interval <interval> last-n <lastn>
(config)# mep 1 dm 1 dual flow interval 1 ?
    last-n    The last N dalays used for average last N calculation. Min value
              is 10.
(config)# mep 1 dm 1 dual flow interval 1 last-n ?
    <uint>    The last N value.
(config)# mep 1 dm 1 dual flow interval 1 ?
    last-n    The last N dalays used for average last N calculation. Min value is 10.
(config)# mep 1 dm 1 dual flow ?
    interval    Interval between PDU transmission in 10ms. Min value is 10.
    multi       OAM PDU is transmitted with multicast MAC.
    uni         OAM PDU is transmitted with unicast MAC. The MAC is taken from
                peer MEP MAC database.
(config)# mep 1 dm 1 dual flow multi ?
    interval    Interval between PDU transmission in 10ms. Min value is 10.
(config)# mep 1 dm 1 dual flow multi interval ?
    <uint>    Interval value.
(config)# mep 1 dm 1 dual flow multi interval 10 ?
    last-n    The last N dalays used for average last N calculation. Min value is 10.
(config)# mep 1 dm 1 dual flow multi interval 10 last-n ?
    <uint>    The last N value.
(config)# do show mep dm

MEP DM state is:

RxTime : Rx Timeout
RxErr :  Rx Error
AvTot :  Average delay Total
AvN :    Average delay last N
Min :    Min Delay value
Max :    Max Delay value
AvVarT : Average delay Variation Total
AvVarN : Average delay Variation last N
MinVar : Min Delay Variation value
MaxVar : Max Delay Variation value
OF  :    Overflow. The number of statistics overflow.

            Inst       Tx       Rx   RxTime    RxErr     AvTot       AvN       Min       Max
AvVarTot   AvVarN    MinVar   MaxVar  OF Unit
1-Way FtoN     1        0        0        0        0         0         0
 0        0         0        0         0        0   0   us
1-Way NtoF     1        0        0        0        0         0         0
 0        0         0        0         0        0   0   us
-- more --, next page: Space, continue: g, quit: ^C
```

Command: Configure Down MEP Domain

Syntax: **mep** <inst> [mip] { up | down } **domain** { port | evc | vlan | tp-link | tunnel-tp | pw | lsp } [vid <vid>] [**flow** <flow>] **level** <level> [**interface** <port_type> <port>]

Description: Configure the enabled MEP domain as:

- **evc** This MEP is a EVC domain MEP.
- **lsp** This MIP is an MPLS-TP LSP domain MIP.
- **port** This MEP is a Port domain MEP.
- **pw** This MEP is an MPLS-TP Pseudo-Wire domain MEP.
- **tp-link** This MEP is an MPLS-TP link domain MEP.
- **tunnel-tp** This MEP is an MPLS-TP tunnel domain MEP.
- **vlan** This MEP is a VLAN domain MEP.

Mode: (config)

Example: Configure an enabled MEP domain. Note: MPLS-TP parameters are not currently supported.

```
(config)# mep 1 down domain evc ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
(config)# mep 1 down domain lsp ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
(config)# mep 1 down domain port ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
(config)# mep 1 down domain pw ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
(config)# mep 1 down domain tp-link ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
(config)# mep 1 down domain tunnel-tp ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
(config)# mep 1 down domain vlan ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
```

```
            Pseudo-Wire domain MEP, the flow instance that the MEP is related
            to must be given.
    level   The MEG level of the MEP.
    vid     In case the MEP is a Port domain Up-MEP or a EVC domain customer
            MIP (on the UNI), the VID must be given.
(config)# mep 1 down domain vlan
```

Command: Configure MEP Loopback

Syntax: **mep** <inst> **lb** <prio> [dei] [multi | { uni { { mep-id <mepid> } | { mac <mac>} } } | mpls ttl <mpls_ttl>] count <count> size <size> interval <interval>

Description: Configure the enabled MEP loopback parameters. The loopback is analogous to the ICMP Ping. Loopback message/Loopback response (LBM/LBR) and is used for fault isolation/detection (not for performance/SLA verification). Each MEP and MIP can be uniquely addressed and individually tested via loopback. A Loopback is initiated by a MEP to check a loop-back path with all peer MEPs in the group.

Mode: (config)#

Example: Configure MEP 1 loopback parameters.

```
(config)# mep 1 lb ?
    <0-7>    Priority in case of tagged OAM. In the MPLS and EVC domain this is
             the COS-ID.
(config)# mep 1 lb 0 ?
    count    The number of LBM PDUs to send in one loop test. The value 0
             indicate infinite transmission (test behaviour). This is HW based
             LBM/LBR and Requires VOE.
    dei      Drop Eligible Indicator in case of tagged OAM.
    mpls     Specify optional values for loopback initiated from an MPLS-TP
             MEP.
    multi    OAM PDU is transmitted with multicast MAC. Not used for MPLS-TP.
    uni      OAM PDU is transmitted with unicast MAC. The MAC is taken from
             peer MEP MAC database. Not used for MPLS-TP.
(config)# mep 1 lb 0 dei ?
    count    The number of LBM PDUs to send in one loop test. The value 0
             indicate infinite transmission (test behaviour). This is HW based
             LBM/LBR and Requires VOE.
    mpls     Specify optional values for loopback initiated from an MPLS-TP
             MEP.
    multi    OAM PDU is transmitted with multicast MAC. Not used for MPLS-TP.
    uni      OAM PDU is transmitted with unicast MAC. The MAC is taken from
             peer MEP MAC database. Not used for MPLS-TP.
(config)# mep 1 lb 0 count ?
    <uint>    Number of LBM PDUs to send value.
(config)# mep 1 lb 0 mpls ?
    ttl    Specify Time-To-Live value to be used for the MPLS-TP OAM LBM PDU.
           Default is to use TTL value 255.
(config)# mep 1 lb 0 multi ?
    count    The number of LBM PDUs to send in one loop test. The value 0
             indicate infinite transmission (test behaviour). This is HW based
             LBM/LBR and Requires VOE.
    dei      Drop Eligible Indicator in case of tagged OAM.
(config)# mep 1 lb 0 uni ?
    mac       Loop Back unicast MAC to be used in case of LB against MIP.
    mep-id    Peer MEP-ID for unicast LB. The MAC is taken from peer MEP MAC
              database. Not used for MPLS-TP.
(config)# mep 1 lb 0 uni
```

Note: the MPLS-TP parameters are not currently supported.

Command: Configure MEP Locked Signal

Syntax: **mep** <inst> **lck** <frame rate>

Description: Configure the enabled MEP Locked Signal parameters. LCK is signaled by peer MEPS to indicate an administrative lock condition. It signals to the MEP that testing may be in progress and so that the MEP can differentiate between an administratively locked and a defect condition. It is often used in conjunction with ETH-TST. A locked MEP transmits LCK frames to its client level MEGs, similar to the way AIS works LCK messages must be sent immediately and then at regular transmission intervals (default = 1/second). LCK default CoS ID should correspond to the CoS which yields the lowest frame loss. LCK is declared immediately upon reception of an LCK PDU, and cleared after 3.5 times the transmission interval.

The Locked Signal is transmitted by a MEP on management demand for administratively locking of a server layer or a sub section of a flow.

Mode: (config)

Example: Display the command options and parameters:

```
(config)# mep 1 lck ?
    fr1m    Frame rate is 1 f/min.
    fr1s    Frame rate is 1 f/s.
    <cr>
(config)#
```

Command: Configure MEP MEG Level

Syntax: **mep** <inst> **level** <level 0-7>

Description: Configure the enabled MEP MEG (Maintenance Entity Group) level value (0-7).

Mode: (config)#

Example: Configure MEP level value and show resulting config.

```
(config)# mep 1 level ?
    <0-7>    The MEG level value.
(config)# mep 1 level 2 ?
    <cr>
(config)# mep 1 level 2
(config)# do show mep 1 detail

MEP state is:
  Inst  cLevel  cMeg  cMep  cAis  cLck cLoop cConf  cSsf  aBlk  aTsf  Peer MEP
cLoc  cRdi cPeriod cPrio
     1   False False False False False False False False False  True         0
True False   False False


MEP Basic Configuration is:
  Inst  Mode  Voe  Vola  Direct                   Port    Dom  Level       Format
Name            Meg id  Mep id   Vid  Flow        Eps
    MAC
     1   Mep  Voe          Down    GigabitEthernet 1/1   Port      2      ITU IC
C                       ICC000MEG0000       1     2     -          0  00-C0-F2-5
6-1A-91

(config)#
```

The MEG Levels per MEF 30 include:

MEG	Suggested Use (MEF 30)	Default Direction for MEPs	Default MEG Level
Subscriber MEG	Subscriber monitoring of an Ethernet service.	Up or Down	6
Test MEG	Service Provider isolation of subscriber reported problems.	Down	5
EVC MEG	Service Provider monitoring of provided service.	Up	4
Service Provider MEG	SP Monitoring of Service Provider network.	Up	3
Operator MEG	Network Operator monitoring of their portion of a network.	Up	2
UNI MEG	Service Provider monitoring of a UNI.	Down	1
ENNI MEG	Network Operators' monitoring of an ENNI.	Down	1

Command: Configure MEP LM (Loss Measurement)

Syntax: **mep** <inst> **lm** <prio> [multi | uni] [single | dual] [fr10s | fr1s | fr6m | fr1m | fr6h] [flr <flr>]
mep <inst> **lm flow-counting**
mep <inst> **lm oam-counting** { [y1731 | all] }
<**0**-**7**> Priority in case of tagged OAM. In the MPLS and EVC domain this is the COS-ID.
flow-counting Loss Measurement is counting service frames per flow - all priority in one.
oam-counting Loss Measurement is counting OAM frames either as Y1731 or all.

Description: Configure the enabled MEP LM (Loss Measurement) parameters for Frame loss measurement (ETH-LM). Loss Measurement is done between MEPs only. There can only be two MEPs in the group – this is a flow point to point functionality. Both the near-end and the far-end loss can be calculated based of the exchanged information between the MEP. Loss measurement is implemented for both CCM based, or LMM/LMR based.

Mode: (config)#

Example 1: Configure the enabled MEP's LM (Loss Measurement) parameters:

```
(config)# mep 1 lm ?
  <Prio : 0-7>  Priority in case of tagged OAM. In the EVC domain this is the COS-ID.
(config)# mep 1 lm 6 ?
    dual      Dual ended LM is based on CCM PDU.
    flr       The Frame Loss Ratio interval.
    fr10s     Frame rate is 10 f/s.
    fr1m      Frame rate is 1 f/min.
    fr1s      Frame rate is 1 f/s.
    fr6h      Frame rate is 6 f/hour.
    fr6m      Frame rate is 6 f/min.
    multi     OAM PDU is transmitted with multicast MAC.
    single    Single ended LM is based on LMM/LMR PDU.
    uni       OAM PDU is transmitted with unicast MAC. The MAC is taken from the
              peer MEP MAC database. In case of LM there is only one peer MEP.
    <cr>
(config)#
```

Example 2: Configure the enabled MEP's LM (Loss Measurement) Flow parameters:

```
(config)# mep 1 lm ?
    <0-7>             Priority in case of tagged OAM. In the MPLS and EVC domain
                      this is the COS-ID.
    flow-counting     Loss Measurement is counting service frames per flow - all
                      priority in one.
    oam-counting      Loss Measurement is counting OAM frames either as Y1731 or
                      all
(config)# mep 1 lm flow-counting ?
    <cr>
(config)# mep 1 lm flow-counting
(config)# do show mep 1

MEP state is:
  Inst  cLevel  cMeg  cMep  cAis  cLck cLoop cConf  cSsf  aBlk  aTsf  Peer MEP
cLoc  cRdi cPeriod cPrio
     1   False False False False False False False False False False

(config)#
```

Example 3: Configure the enabled MEP's LM (Loss Measurement) OAM parameters and show the resulting config:

```
(config)# mep 1 lm flow-counting?
    flow-counting    Loss Measurement is counting service frames per flow - all
                     priority in one.
    <cr>
(config)# mep 1 lm flow-counting?
mep <inst> lm flow-counting
(config)# mep 1 lm oam-counting ?
    all      Loss Measurement is counting all OAM frames as service frames.
    y1731    Loss Measurement is counting OAM frames as service frames as
             described in Y1731.
    <cr>
(config)# mep 1 lm oam-counting all ?
    <cr>
(config)# mep 1 lm oam-counting all
(config)# mep 1 lm oam-counting y1731
(config)# mep 1 lm oam-counting
(config)# end
# show mep lm detail

MEP LM state is:
     Inst     Tx     Rx     Near Count     Far Count     Near Ratio     Far Ratio
        1      0      0              0             0              0      0
        2      0      0              0             0              0      0


MEP LM Configuration is:
     Inst     Prio     Cast      Ended       Rate     Flr  Flow Count   Oam Count
        1                                                      Enable         All
        2                                                     Disable       Y1731

#
```

Command: Configure MEP Link State Tracking

Syntax: **link-state-tracking**

Description: Configure a MEP's Link State Tracking (LST). When LST is enabled in an instance, a Local SF or received 'isDown' in CCM Interface Status TLV will bring down the residence port. Only valid in Up-MEP.

Mode: (config)#

Example: Configure an Up MEP's Link State Tracking (LST).

```
(config)# mep 1 link-state-tracking?
    link-state-tracking    Link State Tracking. When LST is enabled in an
                           instance, Local SF or received 'isDown' in CCM
                           Interface Status TLV, will bring down the residence
                           port. Only valid in Up-MEP.
    <cr>
(config)# mep 1 link-state-tracking ?
    <cr>
(config)# mep 1 link-state-tracking
Error: Invalid parameter error returned from MEP
(config)#
```

Messages:

Error: Invalid parameter error returned from MEP

Error: Invalid number of peer's for this configuration

Command: Configure MEP LT (Link Trace)

Syntax: **mep** <inst> **lt** <prio> { { mep-id <mepid> } | { mac <mac> } } ttl <ttl>

Description: Configure the enabled MEP LT (Link Trace) parameters. Link Trace messages (also called Mac Trace Route) are Multicast frames that a MEP transmits to track the path (hop-by-hop) to a destination MEP. This is similar in concept to UDP Trace Route. Each receiving MEP sends a Trace Route Reply directly to the originating MEP, and regenerates the Trace Route Message.

IEEE802.1 ag support is implemented with the features like Link Trace, Loopback and Continuity Check. Message parameters are framed as per the IEEE standard when the Link Trace feature configuration indicates IEEE Link Trace The LTM (Link Trace Message) PDU is initiated by MEP. MIPs receive and handle the PDU in a manner that allows the MEP to trace the path to the target MAC address. All intermediate MIPs will forward the packet to the egress port for which the target MAC is learnt and at the same time reply to the MEP with a LTR (Link Trace Reply). This continues untill the PDU is received by the management point with the target MAC. This entity does not forward the packet but replies to the originator MEP. The MEP establishes the path by collating all the LTR PDUs.

Mode: (config)#

Example: Show the command functions, confiure an instance and show the resulting config:

```
(config)# mep 1 lt?
    lt    Link Trace.
(config)# mep 1 lt ?
    <0-7>    Priority in case of tagged OAM. In the EVC domain this is the
             COS-ID.
(config)# mep 1 lt?
mep <inst> lt <prio> { { mep-id <mepid> } | { mac <mac> } } ttl <ttl>
(config)# mep 1 lt 4 ?
    mac       Link Trace target unicast MAC to be used in case of LT against
              MIP.
    mep-id    Peer MEP-ID for Link Trace target unicast MAC. The MAC is taken
              from peer MEP MAC database.
(config)# mep 1 lt 4 mac ?
    <mac_addr>    Link Trace target unicast MAC value.
(config)# mep 1 lt 4 mac 11-22-33-44-55-66 ?
    ttl    Time To Live.
(config)# mep 1 lt 4 mac 11-22-33-44-55-66 ttl ?
    <uint>    Time To Live value.
(config)# mep 1 lt 4 mac 11-22-33-44-55-66 ttl 100
(config)# do show mep 1 lt
MEP LT state is:
     Inst   Transaction ID   Ttl   Mode   Direction   Forwarded    relay  Last MAC    Next MAC
        1                1
                         2
                         3
                         4
                         5

(config)#
```

Command: Configure MEP MEG ID

Syntax: **mep** <inst> **meg-id** <megid> { itu | itu-cc | { ieee [name <name>] } }
Description: Configure the enabled MEP's ITU/IEEE MEG-ID string (e.g., "ICC000MEG0000").
Mode: (config)#
Example: Configure the enabled MEG ID and show resulting config.

```
(config)# mep 1 meg-id ?
    <word>    The MEG-ID string. This is either the ITU MEG-ID or the IEEE Short MA,
              depending on the selected MEG-ID format. The ITU max. is 13 characters.
              The ITU-CC max. is 15 characters. The IEEE max. is 16 characters.
(config)# mep 1 meg-id?
    meg-id    The ITU/IEEE MEG-ID.
(config)# mep 1 meg-id?
mep <inst> meg-id <megid> { itu | itu-cc | { ieee [ name <name> ] } }
(config)# mep 1 meg-id?
    meg-id    The ITU/IEEE MEG-ID.
(config)# mep 1 meg-id
```

Command: Configure MEP ID

Syntax: **mep** <inst> **mep-id** <id 1-4095>
Description: Configure the enabled MEP ID value.
Mode: (config)#
Example: Configure the enabled MEP ID and show resulting config.

```
(config)# mep 1 mep-id ?
    <uint>    The MEP-ID value.
(config)# mep 1 mep-id?
    mep-id    The MEP-ID.
(config)# mep 1 mep-id?
mep <inst> mep-id <mepid>
(config)# mep 1 mep-id?
    mep-id    The MEP-ID.
(config)# mep 1 mep-id 444
(config)# do show mep 444

MEP state is:
  Inst  cLevel  cMeg  cMep  cAis  cLck cLoop cConf  cSsf  aBlk  aTsf  Peer MEP
cLoc  cRdi cPeriod cPrio
Error: Invalid MEP instance ID

(config)#
(config)# do show mep 1

MEP state is:
  Inst  cLevel  cMeg  cMep  cAis  cLck cLoop cConf  cSsf  aBlk  aTsf  Peer MEP
cLoc  cRdi cPeriod cPrio
     1   False False False False False False False False False False

(config)#
```

Command: Configure MEP MIP (MEG Intermediate Point)

Syntax: **mep** <inst> [mip] { up | down } domain { port | evc | vlan | tp-link | tunnel-tp | pw | lsp } [vid <vid>] [flow <flow>] level <level> [interface <port_type> <port>]

Description: Configure the enabled MEP MIP (MEG Intermediate Point).

Mode: (config)#

Example: Display down MIP parameters:

```
(config)# mep 1 mip?
    mip    This MEP instance is a half-MIP.
(config)# mep 1 mip ?
    down    This MEP is a Down-MEP.
    up      This MEP is a UP-MEP.
(config)# mep 1 mip?
    mip    This MEP instance is a half-MIP.
(config)# mep 1 mip?
mep <inst> [ mip ] { up | down } domain { port | evc | vlan | tp-link | tunnel-tp | pw | lsp }
[ vid <vid> ] [ flow <flow> ] level <level> [ interface <port_type> <port> ]
(config)# mep 1 mip down ?
    domain    The domain of the MEP.
(config)# mep 1 mip down domain ?
    evc          This MEP is a EVC domain MEP.
    lsp          This MIP is an MPLS-TP LSP domain MIP.
    port         This MEP is a Port domain MEP.
    pw           This MEP is an MPLS-TP Pseudo-Wire domain MEP.
    tp-link      This MEP is an MPLS-TP link domain MEP.
    tunnel-tp    This MEP is an MPLS-TP tunnel domain MEP.
    vlan         This MEP is a VLAN domain MEP.
(config)# mep 1 mip down domain evc ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
(config)# mep 1 mip down domain lsp ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
(config)# mep 1 mip down domain port ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
(config)# mep 1 mip down domain pw ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
(config)# mep 1 mip down domain tp-link ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
```

```
              to must be given.
    level     The MEG level of the MEP.
    vid       In case the MEP is a Port domain Up-MEP or a EVC domain customer
              MIP (on the UNI), the VID must be given.
(config)# mep 1 mip down domain tunnel-tp ?
    flow      In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
              Pseudo-Wire domain MEP, the flow instance that the MEP is related
              to must be given.
    level     The MEG level of the MEP.
    vid       In case the MEP is a Port domain Up-MEP or a EVC domain customer
              MIP (on the UNI), the VID must be given.
(config)# mep 1 mip down domain vlan ?
    flow      In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
              Pseudo-Wire domain MEP, the flow instance that the MEP is related
              to must be given.
    level     The MEG level of the MEP.
    vid       In case the MEP is a Port domain Up-MEP or a EVC domain customer
              MIP (on the UNI), the VID must be given.
(config)# mep 1 mip down domain vlan flow ?
    <uint>    The VLAN, EVC, MPLS-TP link, MPLS-TP tunnel, MPLS-TP LSP or
               MPLS-TP Pseudo-Wire flow instance number.
(config)# mep 1 mip down domain vlan flow 1 ?
    level     The MEG level of the MEP.
    vid       In case the MEP is a Port domain Up-MEP or a EVC domain customer
              MIP (on the UNI), the VID must be given.
(config)# mep 1 mip down domain vlan flow 1 level ?
    <0-7>     The MEG level value.
(config)# mep 1 mip down domain vlan flow 1 level 3 ?
    interface    The recidence port of the MEP.
    <cr>
(config)# mep 1 mip down domain vlan flow 1 level 3 interface ?
    GigabitEthernet       1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
(config)# $ip down domain vlan flow 1 level 3 interface GigabitEthernet ?
    <port_type_id>    Port ID in 1/1-4
(config)# $ip down domain vlan flow 1 level 3 interface GigabitEthernet 1/2
MEP instance is already created - must be deleted first
(config)#
```

Example: Display down MIP parameters:

```
(config)# mep 1 mip up?
    up    This MEP is a UP-MEP.
(config)# mep 1 mip up ?
    domain    The domain of the MEP.
(config)# mep 1 mip up domain ?
    evc     This MEP is a EVC domain MEP.
    port    This MEP is a Port domain MEP.
    vlan    This MEP is a VLAN domain MEP.
(config)# mep 1 mip up domain evc ?
    flow    The flow instance that the MEP is related to.
    vid     In case the MEP is a port Up-MEP or a EVC customer MIP the VID must be given.
(config)# mep 1 mip up domain port ?
    flow    The flow instance that the MEP is related to.
    vid     In case the MEP is a port Up-MEP or a EVC customer MIP the VID must be given.
(config)# mep 1 mip up domain vlan ?
    flow    The flow instance that the MEP is related to.
    vid     In case the MEP is a port Up-MEP or a EVC customer MIP the VID must be given.
(config)# mep 1 mip up domain vlan
```

Note: the MPLS-TP parameters are not currently supported.

Command: Configure MEP Peer MEP ID

Syntax: **mep** <inst> **peer-mep-id** <mepid> [mac <mac>]
Description: Configure the enabled MEP's peer MEP ID value, where:
peer-mep-id : The peer MEP-ID.
mac : The peer MAC. This will be overwritten by any learned MAC via CCM reception.
Mode: (config)#
Example: Configure the enabled peer MEP.

```
(config)# mep 1 peer-mep-id ?
    <uint>    The peer MEP-ID value.
(config)# mep 1 peer-mep-id 2 ?
    mac     The peer MAC. this will be overwritten by any learned MAC - through
            CCM reception.
    <cr>
(config)# mep 1 peer-mep-id 2
(config)# mep 1 peer-mep-id 2 mac ?
    <mac_addr>    The peer MAC string.
(config)# mep 1 peer-mep-id 2 mac 00-00-00-00-00-00 ?
    <cr>
(config)# mep 1 peer-mep-id 2 mac 00-00-00-00-00-00
(config)#
```

Command: Configure MEP Performance Monitoring (PM)

Syntax: **mep** <inst> **performance-monitoring**
Description: Configure the enabled MEP's PM (Performance Monitoring) parameters. Per MEF 35, PM involves the collection of data concerning the performance of the network.
Mode: (config)#
Example: Configure the enabled MEP perf mon.

```
(config)# mep 1 perf?
    performance-monitoring    Performance monitoring Data Set collection (MEF35)
(config)# mep 1 perf ?
    <cr>
(config)# mep 1 perf
This MEP is not enabled
(config)#
(config)# mep 1 performance-monitoring
(config)# end
# show mep 1 detail

MEP state is:
  Inst  cLevel  cMeg  cMep  cAis  cLck cLoop cConf  cSsf  aBlk  aTsf  Peer MEP
cLoc  cRdi cPeriod cPrio
     1   False False False False False False False False False False


MEP Basic Configuration is:
  Inst  Mode  Voe  Vola  Direct                    Port    Dom  Level       Forma
t              Name            Meg id  Mep id   Vid  Flow        Eps
    MAC
     1   Mep              Down    GigabitEthernet 1/1   Port      0      ITU IC
C                       ICC000MEG0000       1    10     -          0  00-C0-F2-5
6-16-D1

#
```

Command: Enable MEP Syslog

Syntax: **mep 1 syslog**

Description: Enable MEP's system logging function.

Mode: (config)#

Example: Enable MEP 1 system logging:

```
(config)# do show mep syslog detail

MEP Syslog Configuration is:
     Inst  enabled
        1    False
        2    False

(config)# mep 1 syslog
(config)# do show mep syslog detail

MEP Syslog Configuration is:
     Inst  enabled
        1     True
        2    False

(config)#
```

Command: Configure MEP Test Signal

Syntax: **mep** <inst> **tst** <prio> [dei] **mep-id** <mepid> **[sequence]** [all-zero | all-one | one-zero] **rate** <rate> **size** <size>

Description: Configure the enabled MEP's Test signal parameters. Test is used between peer MEPS to provide a one-way in-service or out-of-service test. Test can measure throughput, frame-loss, bit errors, etc. Out of service testing is usually preceded by setting the Eth-Lck state. Test default CoS ID should correspond to the CoS which yields the lowest frame loss.

Mode: (config)#

Example: Configure an enabled MEP's TST Signal function:

```
(config)# mep 1 tst ?
    <0-7>    Priority in case of tagged OAM. In the MPLS and EVC domain this is the COS-ID.
    rx       Receive Test Signal.
    tx       Transmit Test Signal.
(config)# mep 1 tst 2 ?
    dei       Drop Eligible Indicator in case of tagged OAM.
    mep-id    Peer MEP-ID for unicast TST. The MAC is taken from peer MEP MAC database.
(config)# mep 1 tst 2 dei ?
    mep-id    Peer MEP-ID for unicast TST. The MAC is taken from peer MEP MAC database.
(config)# mep 1 tst 2 dei mep-id ?
    <Mepid : uint>    Peer MEP-ID value.
(config)# mep 1 tst 2 dei mep-id 1 ?
    all-one     Test pattern is set to all one.
    all-zero    Test pattern is set to all zero.
    one-zero    Test pattern is set to 10101010.
    rate        The TST frame transmission bit rate - in Mega bits pr. second.
                Limit on Caracal is 400 Mbps. Limit on Serval is 1Gbps. This is
                the bit rate of a standard frame without any encapsulation. If
                1 Mbps rate is selected in a EVC MEP, the added tag will give a
                higher bitrate on the wire.
    sequence    Enable sequence number in TST PDU.
(config)# mep 1 tst 2 dei mep-id 1 all-one ?
    rate        The TST frame transmission bit rate - in Mega bits pr. second.
                Limit on Caracal is 400 Mbps. Limit on Serval is 1Gbps. This is
                the bit rate of a standard frame without any encapsulation. If
                1 Mbps rate is selected in a EVC MEP, the added tag will give a
                higher bitrate on the wire.
    sequence    Enable sequence number in TST PDU.
(config)# mep 1 tst 2 dei mep-id 1 all-one rate ?
    <uint>    Transmission rate value.
(config)# mep 1 tst 2 dei mep-id 1 all-one rate 100 ?
    size    The TST frame size. This is entered as the wanted size (in bytes)
            of a un-tagged frame containing TST OAM PDU - including CRC (four
            bytes). 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. Minimum Size is 64 Bytes. Maximum
            Size is 9600 Bytes (1526 for MPLS).
(config)# mep 1 tst 2 dei mep-id 1 all-one rate 100 size 64 ?
    <cr>
(config)# mep 1 tst 2 dei mep-id 1 all-one rate 100 size 64
(config)# mep 1 tst rx
(config)# mep 1 tst tx
Error: Invalid peer MEP ID
(config)# mep 2 tst tx
This MEP is not enabled
(config)#
```

Command: Configure Up MEP

Syntax: **mep** <inst> [mip] { up | down } **domain** { port | evc | vlan | tp-link | tunnel-tp | pw | lsp } [vid <vid>] [**flow** <flow>] **level** <level> [**interface** <port_type> <port>]

Description: Configure the enabled MEP (Maintanance Entity End Point) as an Up MEP. Configure this MEP as an Up MEP for monitoring egress OAM and traffic on the 'Residence Port'.

Mode: (config)#

Example 1: Display the available Up MEP command parameters:

```
(config)# mep 1 up ?
    domain    The domain of the MEP.
(config)# mep 1 up domain ?
    evc          This MEP is a EVC domain MEP.
    lsp          This MIP is an MPLS-TP LSP domain MIP.
    port         This MEP is a Port domain MEP.
    pw           This MEP is an MPLS-TP Pseudo-Wire domain MEP.
    tp-link      This MEP is an MPLS-TP link domain MEP.
    tunnel-tp    This MEP is an MPLS-TP tunnel domain MEP.
    vlan         This MEP is a VLAN domain MEP.
(config)# mep 1 up domain evc ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
(config)# mep 1 up domain lsp ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
(config)# mep 1 up domain port ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
(config)# mep 1 up domain pw ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
(config)# mep 1 up domain tp-link ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
(config)# mep 1 up domain tunnel-tp ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
```

```
(config)# mep 1 up domain vlan ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
(config)# mep 1 up domain vlan
```

Example 2: Configure an Up MEP's parameters:

```
(config)# mep 1 up domain vlan ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
(config)# mep 1 up domain vlan flow ?
    <Flow : uint>    The flow instance number when not in the port domain.
(config)# mep 1 up domain vlan vid ?
    <Vid : vlan_id>    The port Domain MEP VID. This is required for a Port Up-MEP.
(config)# mep 1 up domain vlan vid 1 ?
    flow    The flow instance that the MEP is related to.
(config)# mep 1 up domain vlan vid 1 flow 2 ?
    level    The MEG level of the MEP.
(config)# mep 1 up domain vlan vid 1 flow 2 level ?
    <Level : 0-7>    The MEG level value.
(config)# mep 1 up domain vlan vid 1 flow 2 level 7 ?
    interface    The recidence port of the MEP.
(config)# mep 1 up domain vlan vid 1 flow 2 level 7 interface ?
    GigabitEthernet       1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
(config)# $p domain vlan vid 1 flow 2 level 7 interface GigabitEthernet ?
    PORT_ID    Port ID in 1/1-6
(config)# $p domain vlan vid 1 flow 2 level 7 interface GigabitEthernet 1/1 ?
    <cr>
(config)# $p domain vlan vid 1 flow 2 level 7 interface GigabitEthernet 1/1
Error: VLAN domain is not supported
(config)#
```

Parameters

<**uint**> The flow instance number of the VLAN, EVC, MPLS-TP link, MPLS-TP tunnel, MPLS-TP LSP or MPLS-TP Pseudo-Wire .

<**0-7**> The MEG level value.

<**vlan_id**> The port Domain MEP or EVC domain customer MIP VID.

Note: the MPLS-TP parameters are not currently supported.

Command: Configure MEP VID (VLAN ID)

Syntax: **mep** <inst> **vid**
Description: Configure the enabled MEP's VLAN ID (VID) parameters.
Mode: (config)#
Example: Configure a MEP's VID:

```
(config)# mep 1 vid?
    vid    The MEP VID.
(config)# mep 1 vid ?
    <vlan_id>    The MEP VID value.
(config)# mep 1 vid?
mep <inst> vid <vid>
(config)# mep 1 vid 1
(config)# mep 1 vid 2
(config)#
```

Messages:

Error: VLAN is not created for this VID displays if the VLAN has not yet been created.

MEP instance is already created - must be deleted first Displays if the MEP is already configured.

Command: Configure MIP (MEG Intermediate Point)

Syntax: **mep** <inst> [**mip**] { up | down } **domain** { port | evc | vlan } [vid <vid>] **flow** <flow> level <level> **interface** <port_type> <port>
mep <inst> [**mip**] { up | down } **domain** { port | evc | vlan | tp-link | tunnel-tp | pw | lsp } [vid <vid>] [**flow** <flow>] **level** <level> [**interface** <port_type> <port>]
Description: Configure the enabled MIP (Maintenance Entity Intermediate Point) parameters.
Mode: (config)#
Example: Configure a MIP':

```
config)# mep 2 mip?
    mip    This MEP instance is a half-MIP.
(config)# mep 2 mip ?
    down    This MEP is a Down-MEP.
    up      This MEP is a UP-MEP.
(config)# mep 2 mip??
    mip    This MEP instance is a half-MIP.
(config)# mep 2 mip?
mep <inst> [ mip ] { up | down } domain { port | evc | vlan | tp-link | tunnel-tp | pw | lsp }
[ vid <vid> ] [ flow <flow> ] level <level> [ interface <port_type> <port> ]
(config)# mep 2 mip up domain ?
    evc          This MEP is a EVC domain MEP.
    lsp          This MIP is an MPLS-TP LSP domain MIP.
    port         This MEP is a Port domain MEP.
    pw           This MEP is an MPLS-TP Pseudo-Wire domain MEP.
    tp-link      This MEP is an MPLS-TP link domain MEP.
    tunnel-tp    This MEP is an MPLS-TP tunnel domain MEP.
    vlan         This MEP is a VLAN domain MEP.
(config)# mep 2 mip up domain evc ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
             Pseudo-Wire domain MEP, the flow instance that the MEP is related
             to must be given.
    level    The MEG level of the MEP.
    vid      In case the MEP is a Port domain Up-MEP or a EVC domain customer
             MIP (on the UNI), the VID must be given.
(config)# mep 2 mip up domain lsp ?
    flow     In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
```

```
            Pseudo-Wire domain MEP, the flow instance that the MEP is related
            to must be given.
    level   The MEG level of the MEP.
    vid     In case the MEP is a Port domain Up-MEP or a EVC domain customer
            MIP (on the UNI), the VID must be given.
(config)# mep 2 mip up domain port ?
    flow    In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
            Pseudo-Wire domain MEP, the flow instance that the MEP is related
            to must be given.
    level   The MEG level of the MEP.
    vid     In case the MEP is a Port domain Up-MEP or a EVC domain customer
            MIP (on the UNI), the VID must be given.
(config)# mep 2 mip up domain pw ?
    flow    In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
            Pseudo-Wire domain MEP, the flow instance that the MEP is related
            to must be given.
    level   The MEG level of the MEP.
    vid     In case the MEP is a Port domain Up-MEP or a EVC domain customer
            MIP (on the UNI), the VID must be given.
(config)# mep 2 mip up domain tp-link ?
    flow    In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
            Pseudo-Wire domain MEP, the flow instance that the MEP is related
            to must be given.
    level   The MEG level of the MEP.
    vid     In case the MEP is a Port domain Up-MEP or a EVC domain customer
            MIP (on the UNI), the VID must be given.
(config)# mep 2 mip up domain tunnel-tp ?
    flow    In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
            Pseudo-Wire domain MEP, the flow instance that the MEP is related
            to must be given.
    level   The MEG level of the MEP.
    vid     In case the MEP is a Port domain Up-MEP or a EVC domain customer
            MIP (on the UNI), the VID must be given.
(config)# mep 2 mip up domain vlan ?
    flow    In case the MEP is a VLAN, EVC, MPLS-TP link, tunnel, LSP or
            Pseudo-Wire domain MEP, the flow instance that the MEP is related
            to must be given.
    level   The MEG level of the MEP.
    vid     In case the MEP is a Port domain Up-MEP or a EVC domain customer
            MIP (on the UNI), the VID must be given.
(config)# mep 2 mip up domain vlan
```

Message: *Error: This MIP is not supported*
Example:

```
(config)# $ip down domain port flow 2 level 6 interface GigabitEthernet ?
    PORT_ID    Port ID in 1/1-6
(config)# $ip down domain port flow 2 level 6 interface GigabitEthernet 1/1
Error: This MIP is not supported
(config)#
```

Message: *Error: EVC flow was found invalid*
Example:

```
(config)# $ 1 up domain evc flow 3 level 6 interface 10GigabitEthernet ?
    PORT_ID    Port ID in 1/1-2
(config)# $ 1 up domain evc flow 3 level 6 interface 10GigabitEthernet 1/2
Error: EVC flow was found invalid
(config)#
```

Message*: MPLS-TP not supported*

Command: Configure Monitor (Mirror)

Syntax: **monitor session** <session_number>
[**destination** { interface (<port_type> [<di_list>]) | remote vlan <drvid> reflector-port <port_type> <rportid> }
| **source** { interface (<port_type> [<si_list>]) [both | rx | tx] | remote vlan <srvid> | vlan <source_vlan_list> }
| **intermediate** { interface (<port_type> [<ii_list>]) | remote vlan <irvid> }]

Description: Configure mirror parameters for 'Many to 1' port mirroring. Mirroring is a feature for switched port analysis. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied to a destination port where a network analyzer can be attached to analyze the network traffic.

Remote Mirroring is an extend function of Mirroring. It can extend the destination port to other switch so the administrator can analyze the network traffic on the other switches. If you want to get the tagged mirrored traffic, you have to set VLAN egress tagging as "Tag All" on the reflector port. On the other hand, if you want to get untagged mirrored traffic, you must set VLAN egress tagging as "Untag ALL" on the reflector port.

destination : MIRROR destination interface or VLAN.
intermediate : MIRROR intermediate interface, VLAN.
source : MIRROR source interface, VLAN.

Mode: (config)#

Example: Configure mirror parameters:

```
(config)# monitor session ?
    <1>    MIRROR session number
(config)# monitor session 1 ?
    destination     MIRROR destination interface or VLAN
    intermediate    MIRROR intermediate interface, VLAN
    source          MIRROR source interface, VLAN
    <cr>
(config)# monitor session 1 destination ?
    interface    MIRROR destination interface
    remote       MIRROR destination Remote
(config)# monitor session 1 destination interface ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
(config)# monitor session 1 destination interface 10 ?
    <port_type_list>    Port list in 1/1-4
(config)# monitor session 1 destination interface 10 1/2 ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
    <cr>
(config)# monitor session 1 destination interface 10 1/2
(config)# monitor session 1 intermediate ?
    interface    MIRROR intermediate interface
    remote       MIRROR intermediate Remote
(config)# monitor session 1 intermediate remote ?
    vlan    MIRROR intermediate Remote number
(config)# monitor session 1 intermediate remote vlan ?
    <vlan_id>    Remote MIRROR intermediate RMIRROR VLAN number
(config)# monitor session 1 intermediate remote vlan 10 ?
    <cr>
(config)# monitor session 1 intermediate remote vlan 10
(config)# monitor session 1 source ?
```

```
    interface    MIRROR source interface
    remote       MIRROR source Remote
    vlan         MIRROR source VLAN
(config)# monitor session 1 source interface ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
(config)# monitor session 1 source remote ?
    vlan    Remote MIRROR source RMIRROR VLAN
(config)# monitor session 1 source remote vlan 100
(config)#
```

Mirror Parameters

session: Select session id to configure.
source: The switch is a source node for monitor flow. The source port(s), reflector port and intermediate port(s) are located on this switch.
intermediate: The switch is a forwarding node for monitor flow and the switch is an option node. The object is to forward traffic from source switch to destination switch. The intermediate ports are located on this switch.
destination: The switch is an end node for monitor flow. The destination port(s) and intermediate port(s) are located on this switch.
vid: The VLAN ID points out where the monitor packet will copy to.
reflector-port: The reflector port is a method to redirect the traffic to Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until the Remote Mirroring is disabled. In the stacking mode, you need to select switch ID to select the correct device. If you shut down a port, it cannot be a candidate for reflector port. If you shut down the port which is a reflector port, the remote mirror function cannot work. Note1: The reflector port needs to select only on Source switch type. Note2: The reflector port needs to disable MAC Table learning and STP. Note3: The reflector port is only supported on pure copper ports.
source vlan(s): The S4224 supports VLAN-based Mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs on this field. Note1: The Mirroring session may have either ports or VLANs as sources, but not both.
port: The logical port for the settings contained in the same row.
source: Select mirror mode:
disabled: Neither frames transmitted nor frames received are mirrored.
both: Frames received and frames transmitted are mirrored on the Intermediate/Destination port.
rx only: Frames received on this port are mirrored on the Intermediate/Destination port. Frames transmitted are not mirrored.
tx only: Frames transmitted on this port are mirrored on the Intermediate/Destination port. Frames received are not mirrored.
intermediate: Selects intermediate port. This is designed for Remote Mirroring. The intermediate port is a switch port to connect to other switch. Note: The intermediate port needs to disable MAC Table learning.
destination: Selects the destination port. This is designed for mirror or Remote Mirroring. The destination port is a switch port that you receive a copy of traffic from the source port. Note1: On mirror mode, the device only supports one destination port. Note2: The destination port needs to disable MAC Table learning.

Mirroring Configuration Guideline for All Features

When the switch is running in Remote Mirroring mode, the administrator also needs to check whether or not other features are enabled or disabled. For example, the administrator has not disabled the MSTP on reflector port. All monitor traffic will be blocked on reflector port. All recommended settings are described as follows.

	Impact	reflector port	intermediate port	destination port	Remote Mirroring VLAN
arp_inspection	High	* disabled	* disabled		
acl	Critical	* disabled	* disabled	* disabled	
dhcp_relay	High	* disabled	* disabled		
dhcp_snooping	High	* disabled	* disabled		
ip_source_guard	Critical	* disabled	* disabled	* disabled	
ipmc/igmpsnp	Critical				un-conflict
ipmc/mldsnp	Critical				un-conflict
lacp	Low			o disabled	
lldp	Low			o disabled	
mac learning	Critical	* disabled	* disabled	* disabled	
mstp	Critical	* disabled		o disabled	
mvr	Critical				un-conflict
nas	Critical	* authorized	* authorized	* authorized	
psec	Critical	* disabled	* disabled	* disabled	
qos	Critical	* unlimited	* unlimited	* unlimited	
upnp	Low			o disabled	
mac-based vlan	Critical	* disabled	* disabled		
protocol-based vlan	Critical	* disabled	* disabled		
vlan_translation	Critical	* disabled	* disabled	* disabled	
voice_vlan	Critical	* disabled	* disabled		
mrp	Low			o disabled	
mvrp	Low			o disabled	

Note:

* -- must o -- optional Impact: Critical/High/Low Critical = 5 packets -> 0 packet
High = 5 packets -> 4 packets Low = 5 packets -> 6 packets

Command: Configure MVR (Multicast VLAN Registration)

Syntax: **config mvr**

Description: Configure MVR (Multicast VLAN Registration) parameters. 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. It is allowed to create at maximum 4 MVR VLANs with corresponding channel profile for each Multicast VLAN. The channel profile is defined by the IPMC Profile which provides the filtering conditions. The parameters are:

name : MVR multicast VLAN name (Max 16 characters).

vlan : MVR multicast VLAN list (Max 16 characters).

Mode: (config)

Example 1: Display the MVR functions supported.

```
(config)# mvr?
    mvr     Multicast VLAN Registration configuration
    <cr>
(config)# mvr ?
    name    MVR multicast name
    vlan    MVR multicast vlan
    <cr>
(config)# mvr??
mvr
mvr name <mvr_name> channel <profile_name>
mvr name <mvr_name> frame priority <cos_priority>
mvr name <mvr_name> frame tagged
mvr name <mvr_name> igmp-address <v_ipv4_ucast>
mvr name <mvr_name> last-member-query-interval <ipmc_lmqi>
mvr name <mvr_name> mode { dynamic | compatible }
mvr vlan <v_vlan_list> [ name <mvr_name> ]
mvr vlan <v_vlan_list> channel <profile_name>
mvr vlan <v_vlan_list> frame priority <cos_priority>
mvr vlan <v_vlan_list> frame tagged
mvr vlan <v_vlan_list> igmp-address <v_ipv4_ucast>
mvr vlan <v_vlan_list> last-member-query-interval <ipmc_lmqi>
mvr vlan <v_vlan_list> mode { dynamic | compatible }
(config)# mvr
```

Example 2: Display the MVR parameters.

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

Example 3: Configure MVR name functions.

```
(config)# mvr?
    mvr     Multicast VLAN Registration configuration
    <cr>
(config)# mvr ?
    name    MVR multicast name
    vlan    MVR multicast vlan
    <cr>
(config)# mvr name ?
    <MvrName : word16>    MVR multicast VLAN name
(config)# mvr name MVR1 ?
    channel                       MVR channel configuration
    frame                         MVR control frame in TX
    igmp-address                  MVR address configuration used in IGMP
    last-member-query-interval    Last Member Query Interval in tenths of
                                  seconds
    mode                          MVR mode of operation
(config)# mvr name MVR1 channel ?
    <ProfileName : word16>    Profile name in 16 char's
(config)# mvr name MVR1 channel FirstMVR ?
    <cr>
(config)# mvr name MVR1 channel FirstMVR
% Invalid operation.

% Failed to set MVR interface channel.

(config)# mvr name MVR1 channel FirstMVR ?
    <cr>
(config)# mvr name ?
    <MvrName : word16>    MVR multicast VLAN name
(config)# mvr name MVR1 ?
    channel                       MVR channel configuration
    frame                         MVR control frame in TX
    igmp-address                  MVR address configuration used in IGMP
    last-member-query-interval    Last Member Query Interval in tenths of
                                  seconds
    mode                          MVR mode of operation
(config)# mvr name MVR1 frame ?
    priority    Interface CoS priority
    tagged      Tagged IGMP/MLD frames will be sent
(config)# mvr name MVR1 frame priority ?
    <CosPriority : 0-7>    CoS priority ranges from 0 to 7
(config)# mvr name MVR1 frame priority 0 ?
    <cr>
(config)# mvr name MVR1 frame priority 0
% Invalid MVR VLAN MVR1.

% Failed to set MVR interface priority settings.

(config)# mvr 1 name MVR1 frame ?
            ^
% Invalid word detected at '^' marker.

(config)# mvr name MVR1 ?
    channel                       MVR channel configuration
    frame                         MVR control frame in TX
    igmp-address                  MVR address configuration used in IGMP
    last-member-query-interval    Last Member Query Interval in tenths of
                                  seconds
    mode                          MVR mode of operation
```

```
(config)# mvr name MVR1 igmp-address ?
    <ipv4_ucast>    A valid IPv4 unicast address
(config)# mvr name MVR1 igmp-address 192.168.1.30 ?
    <cr>
(config)# mvr name MVR1 igmp-address 192.168.1.30
% Invalid MVR VLAN MVR1.

% Failed to set MVR IGMP address settings for IGMP.

(config)# mvr name MVR1 last-member-query-interval ?
    <IpmcLmqi : 0-31744>    0 - 31744 tenths of seconds
(config)# mvr name MVR1 last-member-query-interval 400 ?
    <cr>
(config)# mvr name MVR1 last-member-query-interval 400
% Invalid MVR VLAN MVR1.

% Failed to set MVR interface LMQI.

(config)#
```

Example 3: Configure MVR vlan functions.

```
(config)# mvr vlan 1 ?
    channel                      MVR channel configuration
    frame                        MVR control frame in TX
    igmp-address                 MVR address configuration used in IGMP
    last-member-query-interval   Last Member Query Interval in tenths of seconds
    mode                         MVR mode of operation
    name                         MVR multicast name
    <cr>
(config)# mvr vlan 1 channel ?
    <ProfileName : word16>    Profile name in 16 char's
(config)# mvr vlan 1 channel CH1 ?
    <cr>
(config)# mvr vlan 1 channel CH1
% Invalid operation.

% Failed to set MVR interface channel.

(config)# mvr vlan 1 frame ?
    priority    Interface CoS priority
    tagged      Tagged IGMP/MLD frames will be sent
(config)# mvr vlan 1 frame priority ?
    <CosPriority : 0-7>    CoS priority ranges from 0 to 7
(config)# mvr vlan 1 frame priority 0 ?
    <cr>
(config)# mvr vlan 1 frame priority 0
% Invalid MVR VLAN ID 1.

(config)# mvr vlan 1 frame tagged ?
    <cr>
(config)# mvr vlan 1 frame tagged
% Invalid MVR VLAN ID 1.

(config)# mvr vlan 1 igmp-address ?
    <ipv4_ucast>    A valid IPv4 unicast address
(config)# mvr vlan 1 igmp-address 192.168.1.30 ?
    <cr>
(config)# mvr vlan 1 igmp-address 192.168.1.30
% Invalid MVR VLAN ID 1.
```

```
(config)# mvr vlan 1 last-member-query-interval ?
    <IpmcLmqi : 0-31744>    0 - 31744 tenths of seconds
(config)# mvr vlan 1 last-member-query-interval 999 ?
    <cr>
(config)# mvr vlan 1 last-member-query-interval 999
% Invalid MVR VLAN ID 1.

(config)# mvr vlan 1 mode ?
    compatible    Compatible MVR operation mode
    dynamic       Dynamic MVR operation mode
(config)# mvr vlan 1 mode compatible ?
    <cr>
(config)# mvr vlan 1 mode compatible
% Invalid MVR VLAN ID 1.

(config)# mvr vlan 1 mode dynamic ?
    <cr>
(config)# mvr vlan 1 mode dynamic
% Invalid MVR VLAN ID 1.

(config)# mvr vlan 1 name ?
    <MvrName : word16>    MVR multicast VLAN name
(config)# mvr vlan 1 name MVR01
(config)# mvr vlan 1 name?
    name    MVR multicast name
(config)# mvr vlan 1 name
```

Note: The *IpmcLmqi* parameter is the per-VLAN Last Member Query Interval.

MVR Parameters:

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

Command: Configure No

Syntax: **no**

Description: Negate a command or set its defaults. Every configuration command has a “no” form to negate or set its default. In general, the no form is used to reverse the action of a command or reset a value back to the default. For example, the ‘**no ip routing**’ configuration command reverses the ‘**ip routing**’ of an interface.

Mode: (config) or (exec)

Example 1: Exec mode available ***no*** commands.

```
# no ?
    debug     Configure NTP       Debugging functions
    port-security    Port security (psec limit)
    ptp              Enable wireless mode for an interface.
    terminal         Set terminal line parameters
# no
```

Example 2: Config mode available ***no*** commands.

```
(config)# no?
    no    Negate a command or set its defaults
(config)# no ?
    aaa              Authentication, Authorization and Accounting
    access           Access management
    access-list      Access list
    aggregation      Aggregation mode
    banner           Define a login banner
    clock            Configure time-of-day clock
    ddmi             DDMI Information
    debug            Debugging functions
    dot1x            IEEE Standard for port-based Network Access Control
    enable           Modify enable password parameters
    eps              Ethernet Protection Switching.
    erps             Ethernet Ring Protection Switching
    evc              Ethernet Virtual Connections
    gvrp             Enable GVRP feature
    hostname         Set system's network name
    interface        Select an interface to configure
    ip               Internet Protocol
    ipmc             IPv4/IPv6 multicast configuration
    ipv6             IPv6 configuration commands
    lacp             LACP settings
    lldp             LLDP configurations.
    logging          System logging message
    loop-protect     Loop protection configuration
    mac              MAC table entries/configuration
    mep              Maintenance Entity Point
    monitor          Monitoring different system events
    mvr              Multicast VLAN Registration configuration
    ntp              Configure NTP
    port-security    Enable/disable port security globally.
    privilege        Command privilege parameters
    ptp
    qos              Quality of Service
    radius-server    Configure RADIUS
    rmon             Remote Monitoring
    snmp-server      Enable SNMP server
    spanning-tree    STP Bridge
    switchport       vlan - VLAN translation
    tacacs-server    Configure TACACS+
    udld             Disable UDLD configurations on all fiber-optic ports.
    username         Establish User Name Authentication
    vlan             Vlan commands
    web              Web
(config)# no
```

Example 2: Config mode ***no*** command set.

```
no aaa accounting { console | telnet | ssh }
no aaa authentication login { console | telnet | ssh | http }
no aaa authorization { console | telnet | ssh }
no access management
no access management <access_id_list>
no access-list ace <ace_list>
no access-list rate-limiter [ <rate_limiter_list> ]
no aggregation mode
no banner [ motd ]
no banner exec
no banner login
no clock summer-time
no clock timezone
no ddmi
no debug mep <inst> dm tx { dual | single } <prio> [ interval <interval> ] [ synchronized ]
no debug mep <inst> test tx { lb | tst } { <prio> | all } [ dei ] [ all-zero | all-one | one-zero ] [ rate
<rate> ] [ size <size> ]
no debug mep <inst> volatile
no dot1x authentication timer inactivity
no dot1x authentication timer re-authenticate
no dot1x feature { [ guest-vlan ] [ radius-qos ] [ radius-vlan ] }*1
no dot1x guest-vlan
no dot1x guest-vlan supplicant
no dot1x max-reauth-req
no dot1x re-authentication
no dot1x system-auth-control
no dot1x timeout quiet-period
no dot1x timeout tx-period
no enable password [ level <priv> ]
no enable secret { [ 0 | 5 ] } [ level <priv> ]
no eps <inst>
no eps <inst> command
no eps <inst> holdoff
no eps <inst> revertive
no erps <group>
no erps <group> guard
no erps <group> holdoff
no erps <group> mep
no erps <group> revertive
no erps <group> rpl
no erps <group> topology-change propagate
no erps <group> version
no erps <group> vlan
no evc <evc_id>
no evc ece <ece_id>
no gvrp
no gvrp max-vlans <maxvlans>
no gvrp time { [ join-time <jointime> ] [ leave-time <leavetime> ] [ leave-all-time <leavealltime> ] }*1
no hostname
no interface vlan <vlist>
no ip arp inspection
no ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>
no ip arp inspection vlan <in_vlan_list>
no ip arp inspection vlan <in_vlan_list> logging
no ip dhcp excluded-address <low_ip> [ <high_ip> ]
no ip dhcp pool <pool_name>
no ip dhcp relay
no ip dhcp relay information option
no ip dhcp relay information policy
no ip dhcp server
no ip dhcp snooping
no ip dns proxy
no ip domain name
no ip helper-address
no ip http secure-redirect
no ip http secure-server
```

```
no ip igmp host-proxy [ leave-proxy ]
no ip igmp snooping
no ip igmp snooping vlan [ <v_vlan_list> ]
no ip igmp ssm-range
no ip igmp unknown-flooding
no ip name-server [ <order> ]
no ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>
no ip routing
no ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_va
r> <mask_var>
no ip ssh
no ip verify source
no ipmc profile
no ipmc profile <profile_name>
no ipmc range <entry_name>
no ipv6 mld host-proxy [ leave-proxy ]
no ipv6 mld snooping
no ipv6 mld snooping vlan [ <v_vlan_list> ]
no ipv6 mld ssm-range
no ipv6 mld unknown-flooding
no ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> }
no lacp system-priority <v_1_to_65535>
no lldp holdtime
no lldp med datum
no lldp med fast
no lldp med location-tlv altitude
no lldp med location-tlv civic-addr { country | state | county | city | district | block | street |
leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark
| additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-
community-name | p-o-box | additional-code }
no lldp med location-tlv elin-addr
no lldp med location-tlv latitude
no lldp med location-tlv longitude
no lldp med media-vlan-policy <policies_list>
no lldp reinit
no lldp timer
no lldp transmission-delay
no logging host
no logging on
no loop-protect
no loop-protect shutdown-time
no loop-protect transmit-time
no mac address-table aging-time
no mac address-table aging-time <v_0_10_to_1000000>
no mac address-table learning vlan <vlan_list>
no mac address-table static <v_mac_addr> vlan <v_vlan_id> [ interface ( <port_type> [ <v_port_type_list> ]
) ]
no mep <inst>
no mep <inst> ais
no mep <inst> aps
no mep <inst> cc
no mep <inst> ccm-tlv
no mep <inst> client domain { evc | vlan | lsp } flow { <cflow> | all }
no mep <inst> dm
no mep <inst> dm bin fd <num_fd_var>
no mep <inst> dm bin ifdv <num_ifdv_var>
no mep <inst> dm bin threshold <threshold_var>
no mep <inst> dm ns
no mep <inst> dm overflow-reset
no mep <inst> dm proprietary
no mep <inst> dm syncronized
no mep <inst> lb
no mep <inst> lck
no mep <inst> link-state-tracking
no mep <inst> lm
no mep <inst> lm flow-counting
no mep <inst> lm oam-counting { [ y1731 | all ] }
no mep <inst> lt
no mep <inst> peer-mep-id { <mepid> | all }
```

```
no mep <inst> performance-monitoring
no mep <inst> syslog
no mep <inst> tst rx
no mep <inst> tst tx
no mep <inst> vid
no mep <inst> voe
no monitor session <session_number> [ destination { interface ( <port_type> [ <di_list> ] ) | remote vlan
<drvid> reflector-port } | source { interface ( <port_type> [ <si_list> ] ) [ both | rx | tx ] | remote
vlan <srvid> | vlan <source_vlan_list> } | intermediate { interface ( <port_type> [ <ii_list> ] ) | remote
vlan <irvid> } ]
no mvr
no mvr name <mvr_name> channel
no mvr name <mvr_name> frame priority
no mvr name <mvr_name> frame tagged
no mvr name <mvr_name> igmp-address
no mvr name <mvr_name> last-member-query-interval
no mvr name <mvr_name> mode
no mvr vlan <v_vlan_list>
no mvr vlan <v_vlan_list> channel
no mvr vlan <v_vlan_list> frame priority
no mvr vlan <v_vlan_list> frame tagged
no mvr vlan <v_vlan_list> igmp-address
no mvr vlan <v_vlan_list> last-member-query-interval
no mvr vlan <v_vlan_list> mode
no network-clock clk-source <clk_list> nominate
no network-clock clk-source <clk_src> aneg-mode
no network-clock clk-source <clk_src> hold-timeout
no network-clock clk-source <clk_src> priority
no network-clock clk-source <clk_src> ssm-overwrite
no network-clock input-source
no network-clock option
no network-clock output-source
no network-clock selector
no network-clock ssm-freerun
no network-clock ssm-holdover
no network-clock wait-to-restore
no ntp
no ntp server <index_var>
no port-security
no port-security aging
no port-security aging time
no privilege <mode_name> level <0-15> <cmd>
no ptp <clockinst> clk
no ptp <clockinst> domain
no ptp <clockinst> filter
no ptp <clockinst> ho
no ptp <clockinst> log
no ptp <clockinst> mode { boundary | e2etransparent | p2ptransparent | master | slave | bcfrontend }
no ptp <clockinst> priority1
no ptp <clockinst> priority2
no ptp <clockinst> servo ad
no ptp <clockinst> servo ai
no ptp <clockinst> servo ap
no ptp <clockinst> servo displaystates
no ptp <clockinst> uni <idx>
no ptp ext-clock { output | input }
no ptp system-time
no qos map cos-dscp <cos> dpl <dpl>
no qos map dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 |
af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }
no qos map dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 |
af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }
no qos map dscp-egress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 |
af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } <dpl>
no qos map dscp-ingress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 |
af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }
no qos qce <qce_id_range>
no qos wred group <group> queue <queue> dpl <dpl>
no radius-server attribute 32
```

```
no radius-server attribute 4
no radius-server attribute 95
no radius-server deadtime
no radius-server host <host_name> [ auth-port <auth_port> ] [ acct-port <acct_port> ]
no radius-server key
no radius-server retransmit
no radius-server timeout
no rmon alarm <id>
no rmon event <id>
no snmp-server
no snmp-server access <group_name> model { v1 | v2c | v3 | any } level { auth | noauth | priv }
no snmp-server community v2c
no snmp-server community v3 <community>
no snmp-server contact
no snmp-server engined-id local
no snmp-server host <conf_name>
no snmp-server location
no snmp-server security-to-group model { v1 | v2c | v3 } name <security_name>
no snmp-server trap
no snmp-server user <username> engine-id <engineID>
no snmp-server version
no snmp-server view <view_name> <oid_subtree>
no spanning-tree edge bpdu-filter
no spanning-tree edge bpdu-guard
no spanning-tree mode
no spanning-tree mst <instance> priority
no spanning-tree mst <instance> vlan
no spanning-tree mst forward-time
no spanning-tree mst max-age
no spanning-tree mst max-hops
no spanning-tree mst name
no spanning-tree recovery interval
no spanning-tree transmit hold-count
no switchport vlan mapping <gid> <vlan_list>
no tacacs-server deadtime
no tacacs-server host <host_name> [ port <port> ]
no tacacs-server key
no tacacs-server timeout
no udld { aggressive | enable }
no username <username>
no vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h }
<pid> } | { llc <dsap> <ssap> } } [ group <word16> ]
no vlan { { ethertype s-custom-port } | <vlan_list> }
no web privilege group [ <group_name> ] level
(config)# no
```

Command: Configure NTP Server

Syntax: **ntp server** <index_var> ip-address { <ipv4_var> | <ipv6_var> | <name_var> }

Description: Configure one or more NTP Servers (up to five). Network Time Protocol is widely used to synchronize system clocks among a set of distributed time servers and clients. The implemented NTP version is v4. NTP is disabled by default. The NTP IPv4 or IPv6 address can be configured and a maximum of five NTP servers is supported.
Provide the IPv4 or IPv6 address of a NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating 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 appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'. In addition, it can also accept a domain name address.

Mode: (config)#

Example: Configure an NTP Server and show resulting config:

```
(config)# ntp?
    ntp     Configure NTP
    <cr>
(config)# ntp ?
    server    Configure NTP server
    <cr>
(config)# ntp?
    ntp     Configure NTP
    <cr>
(config)# ntp??
ntp
ntp server <index_var> ip-address { <ipv4_var> | <ipv6_var> | <name_var> }
(config)# ntp server ?
    <1-5>    index number
(config)# ntp server 1 ?
    ip-address    ip address
(config)# ntp server 1 ip-address 192.168.1.30 ?
    <cr>
(config)# ntp server 1 ip-address 192.168.1.30
(config)# end
# show n?
    network-clock    Show selector state.
    ntp              Configure NTP
# show ntp ?
    status    status
# show ntp status ?
    <cr>
# show ntp status
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: Configure Perf-Mon (Perf ormance Monitor)

Syntax: **interval** Measurement Interval
session Session Enabled
storage Storage Enabled

Description: Configure PM Interval, Session, Storage, and Transfer Mode parameters.
perf-mon interval { lm | dm | evc } <minutes_var>
perf-mon session [lm | dm | evc]
perf-mon storage [lm | dm | evc | dm-binning]
perf-mon transfer
perf-mon transfer fixed-offset <fixed_offset_var>
perf-mon transfer hour <hours_var>
perf-mon transfer incomplete
perf-mon transfer minute <minutes_var>
perf-mon transfer mode { all | new | fixed <number_of_fixed_var> }
perf-mon transfer random-offset <random_offset_var>
perf-mon transfer url <url_var>

Mode: (config)#

Example: Configure the various performance monitor parameters:

```
(config)# perf-mon ?
    interval    Measurement Interval
    session     Session Enabled
    storage     Storage Enabled
    transfer    Transfer Mode Enabled
(config)# perf-mon interval ?
    dm     Delay Measurement
    evc    EVC
    lm     Loss Measurement
(config)# perf-mon interval dm ?
    <1-60>    Number of minutes
(config)# perf-mon interval dm 3 ?
    <cr>
(config)# perf-mon interval dm 3
(config)# perf-mon session ?
    dm      Delay Measurement
    evc     EVC
    lm      Loss Measurement
    <cr>
(config)# perf-mon session evc ?
    <cr>
(config)# perf-mon session evc
(config)# perf-mon storage ?
    dm            Delay Measurement
    dm-binning    Delay Measurement Bins
    evc           EVC
    lm            Loss Measurement
    <cr>
(config)# perf-mon storage dm-binning ?
    <cr>
(config)# perf-mon storage dm-binning
(config)# perf-mon transfer ?
    fixed-offset     Scheduled offset
    hour             Scheduled hours
    incomplete       Include intervals from previous incomplete transfers
    minute           Scheduled minutes
    mode             Interval mode
    random-offset    Random offset
    url              Server URL
    <cr>
(config)# perf-mon transfer mode ?
```

```
    all      All available intervals
    fixed    Fixed number of intervals
    new      New intervals since last transfer
(config)# perf-mon transfer mode all ?
    <cr>
(config)# perf-mon transfer mode all
(config)# perf-mon transfer url ?
    <word64>    Server URL (http or tftp)
(config)# perf-mon transfer url 192.168.1.30
(config)# end
# show perf-mon ?
    current          Current interval ID
    interval-id      Specific interval
    interval-info    Measurement interval information
# show perf-mon interval-info
#
```

Command: Configure Port Security

Syntax: **port-security**
port-security aging
port-security aging time <v_10_to_10000000>

Description: Configure port security - enable/disable port security globally. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

time Time in seconds between checks for activity on learned MAC addresses. The valid range is 10 to 10000000 seconds. The default is 3600 seconds (600 minutes or 10 hours).

Mode: (config)#

Example:

```
(config)# port-security ?
    aging    Enable/disable port security aging.
    <cr>
(config)# port-security aging ?
    time    Time in seconds between check for activity on learned MAC
            addresses.
    <cr>
(config)# port-security aging time ?
    <10-10000000>    seconds
(config)# port-security aging
(config)# port-security aging time 500000
(config)#
```

Command: Configure Privilege Level

Syntax: **privilege** { exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-profile } level <privilege> **<cmd>**

Description: Configure CLI command privilege parameters.You can set privilege attributes to each command. A user cannot access or execute a command unless the logged in user has sufficient priveleges assigned. (Not to be confused with User Exec mode and Privileged EXEC mode priveleges.) Before executing a command, the CLI checks that the current mode is still valid, that the user has sufficient privilege, among others.

<0-15> Privilege level, where level 15 allows use of all CLI commands.

Mode: (config)#

Example:

```
(config)# priv?
    privilege    Command privilege parameters
(config)# privilege ?
    config-vlan        VLAN Configuration Mode
    configure          Global configuration mode
    dhcp-pool          DHCP Pool Configuration Mode
    exec               Exec mode
    if-vlan            VLAN Interface Mode
    interface          Port List Interface Mode
    ipmc-profile       IPMC Profile Mode
    line               Line configuration mode
    snmps-host         SNMP Server Host Mode
    stp-aggr           STP Aggregation Mode
(config)# privilege line level 11 ?
    LINE    Initial valid words and literals of the command to modify, in 128
            char's
(config)# privilege config-vlan ?
    level    Set privilege level of command
(config)# privilege config-vlan level ?
    <0-15>    Privilege level
(config)# privilege config-vlan level 12 ?
    LINE    Initial valid words and literals of the command to modify, in 128
            char's
(config)# privilege config-vlan level 12
```

Multiple users can be created on the switch identified by the username and Privilege level.

The privilege level of the user allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, that is it will grant the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group.

By default setting, most groups' privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults, etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

The name identifying the privilege group is called the Group name. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one.

Note: This feature only works for web users. See the *S4224 Web User Guide* for details.

The following description defines these privilege level groups in details:

1. **System**: Contact, Name, Location, Timezone, Log.
2. **Security**: Authentication, System Access Management, Port (contains Dot1x port, MAC-based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and IP source guard.
3. **IP**: Everything except 'ping'.
4. **Port**: Everything except 'VeriPHY'.
5. **Diagnostics**: 'ping' and 'VeriPHY'.
6. **Maintenance**: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.
7. **Debug**: Only present in CLI.

Every group has an authorization Privilege level for the following sub groups and are configurable from 1 to 15:

- configuration read-only (cro)
- configuration/execute read-write (crw)
- status/statistics read-only (sro)
- status/statistics read-write (e.g. for clearing of statistics) (srw)

User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

Command: Configure PTP System Time

Syntax: **ptp system-time**

Description: Enable or disable synchronization between PTP time and system time.

Mode: (config)#

Example: Use the varous configure **ptp system time** command functions and show results:

```
(config)# ptp ?
    <0-3>          Clock instance [0-3]
    ext-clock      Modify external clock configuration
    system-time    Enable synchronization between PTP time and system time
    tc-internal    Define the internal mode used in TC's
(config)# ptp system-time ?
    get    Get (update) the PTP time from the system time
    set    Set (update) the system time from the PTP time
 (config)# ptp system-time get ?
    <cr>
(config)# ptp system-time get
System clock synch mode (Get PTP time from System time)
(config)# ptp system-time set ?
    <cr>
(config)# ptp system-time set
System clock synch mode (Set System time from PTP time)
 (config)# end
# show ptp ?
    <0-3>          Show various PTP data
    ext-clock      Show the external clock configuration.
    system-time    Show the PTP <-> system time synchronization mode.
# show ptp system-time
System clock synch mode (Set System time from PTP time)
#
```

Note: You can click the **Synchronize to System Clock** button to synchronize the System Clock to the PTP Time. Select the Clock Type in RFC2544/Y.1564: The delay measurements in RFC2544 and Y.1564 are always done in the IEEE 1588 domain. There is only one timestamping domain which is the 1588. You can synchronize to/from the system time via the Web GUI (at the **Configuration** > **PTP** menu path) or via the CLI (using the **ptp system-time set** command at the (config) # prompt).

Command: Configure PTP Clock Instance

Syntax: **ptp**

Description: Configure the IEEE 1588 PTP parameters. PTP (IEEE 1588-2008 or 3 version 2) technology used for distribution of frequency and time of day (ToD). The major PTP functions include:

clk	Set PTP slave clock options
domain	Clock domain for PTP.
filter	Set filter parameters.
ho	Set PTP Servo holdover parameters.
log	Set the PTP debug mode.
mode	Enable a PTP instance.
priority1	Clock priority 1 for PTP BMC algorithm (0 is highest priority).
priority2	Clock priority 2 for PTP BMC algorithm (0 is highest priority).
servo	Set Servo parameters.
slave-cfg	Set PTP clock Slave Configuration.
time-property	Set time properties.
uni	Set a Unicast Slave configuration entry.

Mode: (config)#

Example 1: Display the major PTP configurable functions.

```
(config)# ptp?
    ptp    Precision time Protocol (1588)
(config)# ptp ?
    <Clockinst : 0-3>    Clock instance [0-3]
    ext-clock            Modify external clock configuration
    tc-internal          Define the internal mode used in TC's
(config)# ptp
```

Example 2: Display the configurable PTP instance functions.

```
(config)# ptp 0 ?
    clk              Set PTP slave clock options
    domain           Clock domain for PTP
    filter           Set filter parameters
    ho               Set PTP Servo holdover parameters
    log              Set the PTP debug mode
    mode             Enable a PTP instance
    priority1        Clock priority 1 for PTP BMC algorithm (0 is highest priority)
    priority2        Clock priority 2 for PTP BMC algorithm (0 is highest priority)
    servo            Set Servo parameters
    slave-cfg        Set PTP clock Slave Configuration
    time-property    Set time properties
    uni              Set a Unicast Slave configuration entry
(config)# ptp 0
```

The Precision Time Protocol (PTP) is used to synchronize clocks throughout a computer network. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems.

PTP was originally defined in the IEEE 1588-2002 standard, officially entitled "Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems" and published in 2002. In 2008 a revised standard, IEEE 1588-2008 was released. This new version, also known as PTP

Version 2, improves accuracy, precision and robustness but is not backwards compatible with the original 2002 version.

PTP is designed to fill a niche not well served by either of the two dominant protocols (NTP and GPS). PTP is designed for local systems requiring accuracies beyond those attainable using NTP, and also for applications for which a GPS receiver at each node is too costly, or for which GPS signals are inaccessible.

The IEEE 1588 standards describe a hierarchical master-slave architecture for clock distribution. Here, a time distribution system consists of one or more communication media (network segments), and one or more clocks.

An “ordinary clock” is a device with a single network connection and is either the source of (master) or destination for (slave) a synchronization reference.

A “boundary clock” has multiple network connections and can accurately bridge synchronization from one network segment to another. A synchronization master is selected for each of the network segments in the system.

The “grandmaster” is the root timing reference. The grandmaster transmits synchronization information to the other clocks residing on its network segment. Boundary clocks with a presence on that segment then relay accurate time to the other segments to which they are also connected.

IEEE 1588-2008 introduces a clock associated with network equipment used to convey PTP messages. The transparent clock modifies PTP messages as they pass through the device. Timestamps in the messages are corrected for time spent traversing the network equipment. This scheme improves distribution accuracy by compensating for delivery variability across the network. PTP typically uses the same epoch as Unix time (Midnight, 1 January 1970). Where Unix time is based on Coordinated Universal Time (UTC) and is subject to leap seconds, PTP is based on International Atomic Time (TAI) and moves forward monotonically. The PTP grandmaster communicates the current offset between UTC and TAI, so that UTC can be computed from the received PTP time.

Command: Configure PTP Clock SyncE

Syntax: **ptp** <clockinst> **clk sync** <threshold> **ap** <ap>

Description: Configure the IEEE 1588 PTP Slave clock parameters for an existing clock instance.

This command sets the PTP slave clock option to"'clock is SyncE locked". **Note**: the SyncE feature is not supported at S4224 version 2.2.

The PTP command parameters are:

ptp <clockinst> : The clock instance number (0-3).

clk sync <threshold> : Threshold in ns for offsetFromMaster defines when the offset increment/decrement mode is entered (1-1000).

ap <ap> : The offset increment/decrement adjustment factor (1-40).

Mode: (config)#

Example 1: Display the configurable parameters.

```
(config)# ptp 0 clk ?
    sync    Set PTP slave clock options to 'clock is SyncE locked'
(config)# ptp 0 clk sync ?
    <Threshold : 1-1000>    [1..1000] Threshold in ns for offsetFromMaster
                            defines when the offset increment/decrement mode is
                            entered
(config)# ptp 0 clk sync 200 ?
    ap    Set the adjustment factor
(config)# ptp 0 clk sync 200 ap ?
    <Ap : 1-40>    [1..40]  The offset increment/decrement adjustment factor
(config)# ptp 0 clk sync 200 ap 20 ?
    <cr>
(config)# ptp 0 clk sync 200 ap 20
(config)# end
# show ptp 0 clk
Option  threshold  'P'constant
------  ---------  -----------
synce    200        20
#
```

Command: Configure PTP Clock Domain

Syntax: **ptp** <clockinst> **domain** <domain>

Description: Configure the Clock domain for IEEE 1588 PTP. The valid range is 0-127. The default is 1. The "domain" is an interacting set of clocks that synchronize to one another using PTP. Clocks are assigned to a domain by virtue of the contents of the *Subdomain name* (IEEE 1588-2002) or the *domainNumber* (IEEE 1588-2008) fields in the PTP messages they receive or generate. "Subdomains" allow multiple clock distribution systems to share the same communications medium.

Mode: (config)#

Example 1: Configure PTP instance 0 clock domain:

```
(config)# ptp 0 domain ?
    <Domain : 0-127>    PTP domain: range = 0-127
(config)# ptp 0 domain 1 ?
    <cr>
(config)# ptp 0 domain 1
(config)#
```

Command: Configure PTP Filter

Syntax: **ptp** <clockinst> **filter** [delay <delay>] [period <period>] [dist <dist>]

Description: Configure the IEEE 1588 PTP filter parameters.

Mode: (config)#

Example 1: Configure PTP instance 0 filter:

```
(config)# ptp 0 filter ?
    delay     Set delay filter parameter
    dist      Set offset filter dist parameter
    period    Set offset filter period parameter
    <cr>
(config)# ptp 0 filter delay ?
    <0-6>    Log2 of timeconstant in delay lowpass filter, valid range: 1-6,
             Setting the value to 0 means use the same filter function as for
             the offset measurement, in this case the delay filter uses the
             'period' and 'dist' parameters.
(config)# ptp 0 filter dist ?
    <1-10>    Distance between servo update n number of measurement periods,
              valid range: 1-10
(config)# ptp 0 filter period ?
    <1-10000>    Measurement period in number of sync events, valid range:
                 1-10000
(config)# ptp 0 filter delay 1 dist 1 period 100
(config)#
```

Command: Configure PTP Servo Holdover (HO)

Syntax: **ptp** <clockinst> **ho** [filter <ho_filter>] [adj-threshold <adj_threshold>]

Description: Configure the IEEE 1588 PTP Servo holdover parameters.

Mode: (config)#

Example 1: Configure PTP instance 0 servo HO parameters:

```
(config)# ptp 0 ho?
    ho      Set PTP Servo holdover parameters
    <cr>
(config)# ptp 0 ho ?
    adj-threshold    Set adjustment threshold
    filter           Set stabilization period
    <cr>
(config)# ptp 0 ho adj-threshold ?
    <1-1000>    [1..1000]  max frequency adjustment change within the holdover
                stabilization period (ppb*10)
(config)# ptp 0 ho adj-threshold 500 ?
    filter    Set stabilization period
    <cr>
(config)# ptp 0 ho adj-threshold 500 filter ?
    <60-86400>    [60..86400] Holdover filter and stabilization period
(config)# ptp 0 ho adj-threshold 500 filter 900 ?
    <cr>
(config)# ptp 0 ho adj-threshold 500 filter 900
 (config)#
```

Command: Configure PTP Debug Log Mode

Syntax: **ptp** <clockinst> **log** <debug_mode>

Description: Configure the IEEE 1588 PTP Debug Log mode.

Mode: (config)#

Example 1: Configure PTP instance 0 debug log mode:

```
(config)# ptp 0 log ?
    <DebugMode : 1-4>    1-4 Debug log mode, 1 => log offset from master, 2 =>
                         log sync packets, 3 => log Delay_req, 4 => log both
(config)# ptp 0 log 1 ?
    <cr>
(config)# ptp 0 log 4
(config)# ptp 0 log 3
(config)#
```

Command: Configure PTP Mode

The Precision Time Protocol (PTP) is a network protocol for synchronizing computer systems' clocks.

Precise time information is especially important for distributed systems in automation technology. With PTP as described in IEEE 1588, it is possible to synchronize distributed clocks to an accuracy of less than 1 microsecond on Ethernet networks. The demands on the local clocks and the network and computing capacity are relatively low.

Two effects are evident when setting or synchronizing clocks: 1) independent clocks initially run at an "offset". To synchronize them, the less accurate clock is set to the more accurate one (offset correction).

2) real clocks do not run at exactly the same speed. Therefore, the speed of the less accurate clock has to be regulated constantly (drift correction).

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.

Syntax: **ptp** <clockinst> **mode** { boundary | e2etransparent | p2ptransparent | master | slave } [onestep | twostep] [ethernet | ip4multi | ip4unicast | oam | onepps] [oneway | twoway] [id <v_clock_id>] [vid <vid> [<prio>] [tag]] [mep <mep_id>]

Description: Configure the IEEE 1588 PTP mode / parameters.

bcfrontend Boundary Clock frontend. The BC frontend mode allows an external CPU to run the PTP protocol and use the switch/PHY to do the timestamping. A frontend port will timestamp Sync packets egressing the port (i.e., update the correction field). Delay request packets ingressing will have the arrival timestamp attached to the packet.

boundary : Ordinary / Boundary clock. Select Ord-Bound mode to identify the switch port that is connected to a device with the most precise clock. This is the default clock mode. The device is synchronized with the grand-master clock and operates as a parent master clock. This mode is used for switch ports when overload or heavy load conditions produce significant delay jitter.

e2etransparent : End to end transparent clock. Select E2e Transp mode for the switch to synchronize all switch ports with the grand master clock. The switch corrects for the delay incurred by every packet passing through it (this delay is called 'residence time'). E2e Transp mode causes less jitter and error accumulation than boundary mode.

master : Master only clock.

p2ptransparent : Peer to peer transparent clock.

slave : Slave only clock.

Mode: (config)#

Example 1: Display the various PTP mode command functions:

```
(config)# ptp 0 mode bcfrontend ?
    ethernet          Ethernet protocol encapsulation
    ethernet-mixed    Ethernet protocol encapsulation using mix of unicast and
                      multicast
    id                define PTP clock instance identifier
    ip4mixed          IPv4 mixed multicast/unicast protocol encapsulation
    ip4multi          IPv4 multicast protocol encapsulation
    ip4unicast        IPv4 unicast protocol encapsulation
    mep               Define mep id used in OAM based PTP
    oam               OAM encapsulation (only used in Serval based Distributed TC)
    onepps            1PPS master slave synchronization (only used wht Gen2 1588 PHY's)
    onestep           Onestep mode
    oneway            Oneway slave mode (no Delay_req)
    twostep           Twostep mode
    twoway            Twoway slave mode
    vid               define Vlan ID
    <cr>
(config)# ptp 0 mode bcfrontend?
    bcfrontend    Boundary Clock frontend
    <cr>
(config)# ptp 0 mode bcfrontend?
ptp <clockinst> mode { boundary | e2etransparent | p2ptransparent | master | slave | bcfrontend } [
onestep | twostep ] [ ethernet | ethernet-mixed | ip4multi | ip4mixed | ip4unicast | oam | onepps ]
[ oneway | twoway ] [ id <v_clock_id> ][ vid <vid> [ <prio> ] [ tag ] ] [ mep <mep_id> ]
(config)# ptp 0 mode bcfrontend?
    bcfrontend    Boundary Clock frontend
    <cr>
(config)# ptp 0 mode bcfrontend
(config)# ptp 0 mode boundary ?
    ethernet          Ethernet protocol encapsulation
    ethernet-mixed    Ethernet protocol encapsulation using mix of unicast and
                      multicast
    id                define PTP clock instance identifier
    ip4mixed          IPv4 mixed multicast/unicast protocol encapsulation
    ip4multi          IPv4 multicast protocol encapsulation
    ip4unicast        IPv4 unicast protocol encapsulation
    mep               Define mep id used in OAM based PTP
    oam               OAM encapsulation (only used in Serval based Distributed
                      TC)
    onepps            1PPS master slave synchronization(only used wht Gen2 1588
                      PHY's)
    onestep           Onestep mode
    oneway            Oneway slave mode (no Delay_req)
    twostep           Twostep mode
    twoway            Twoway slave mode
    vid               define Vlan ID
    <cr>
(config)# ptp 0 mode e2etransparent ?
    ethernet          Ethernet protocol encapsulation
    ethernet-mixed    Ethernet protocol encapsulation using mix of unicast and
                      multicast
    id                define PTP clock instance identifier
    ip4mixed          IPv4 mixed multicast/unicast protocol encapsulation
    ip4multi          IPv4 multicast protocol encapsulation
    ip4unicast        IPv4 unicast protocol encapsulation
    mep               Define mep id used in OAM based PTP
    oam               OAM encapsulation (only used in Serval based Distributed
                      TC)
    onepps            1PPS master slave synchronization(only used wht Gen2 1588
```

```
                    PHY's)
    onestep         Onestep mode
    oneway          Oneway slave mode (no Delay_req)
    twostep         Twostep mode
    twoway          Twoway slave mode
    vid             define Vlan ID
    <cr>
(config)# ptp 0 mode master ?
    ethernet        Ethernet protocol encapsulation
    ethernet-mixed  Ethernet protocol encapsulation using mix of unicast and
                    multicast
    id              define PTP clock instance identifier
    ip4mixed        IPv4 mixed multicast/unicast protocol encapsulation
    ip4multi        IPv4 multicast protocol encapsulation
    ip4unicast      IPv4 unicast protocol encapsulation
    mep             Define mep id used in OAM based PTP
    oam             OAM encapsulation (only used in Serval based Distributed
                    TC)
    onepps          1PPS master slave synchronization(only used wht Gen2 1588
                    PHY's)
    onestep         Onestep mode
    oneway          Oneway slave mode (no Delay_req)
    twostep         Twostep mode
    twoway          Twoway slave mode
    vid             define Vlan ID
    <cr>
(config)# ptp 0 mode p2ptransparent ?
    ethernet        Ethernet protocol encapsulation
    ethernet-mixed  Ethernet protocol encapsulation using mix of unicast and
                    multicast
    id              define PTP clock instance identifier
    ip4mixed        IPv4 mixed multicast/unicast protocol encapsulation
    ip4multi        IPv4 multicast protocol encapsulation
    ip4unicast      IPv4 unicast protocol encapsulation
    mep             Define mep id used in OAM based PTP
    oam             OAM encapsulation (only used in Serval based Distributed
                    TC)
    onepps          1PPS master slave synchronization(only used wht Gen2 1588
                    PHY's)
    onestep         Onestep mode
    oneway          Oneway slave mode (no Delay_req)
    twostep         Twostep mode
    twoway          Twoway slave mode
    vid             define Vlan ID
    <cr>

(config)# ptp 0 mode slave ?
    ethernet        Ethernet protocol encapsulation
    ethernet-mixed  Ethernet protocol encapsulation using mix of unicast and
                    multicast
    id              define PTP clock instance identifier
    ip4mixed        IPv4 mixed multicast/unicast protocol encapsulation
    ip4multi        IPv4 multicast protocol encapsulation
    ip4unicast      IPv4 unicast protocol encapsulation
    mep             Define mep id used in OAM based PTP
    oam             OAM encapsulation (only used in Serval based Distributed
                    TC)
    onepps          1PPS master slave synchronization(only used wht Gen2 1588
                    PHY's)
    onestep         Onestep mode
    oneway          Oneway slave mode (no Delay_req)
```

```
    twostep           Twostep mode
    twoway            Twoway slave mode
    vid               define Vlan ID
    <cr>
(config)# ptp 0 mode slave ip4mixed ?
    id          define PTP clock instance identifier
    mep         Define mep id used in OAM based PTP
    onestep     Onestep mode
    oneway      Oneway slave mode (no Delay_req)
    twostep     Twostep mode
    twoway      Twoway slave mode
    vid         define Vlan ID
    <cr>

(config)# ptp 0 mode slave mep ?
    <1-100>     Mep instance number used if the OAM protocol option is used
                (only relevant in Serval)
(config)# ptp 0 mode slave vid 100 ?
    <0-7>             The range of Priorities ptp can use in the tagged frames
    ethernet          Ethernet protocol encapsulation
    ethernet-mixed    Ethernet protocol encapsulation using mix of unicast and multicast
    id                define PTP clock instance identifier
    ip4mixed          IPv4 mixed multicast/unicast protocol encapsulation
    ip4multi          IPv4 multicast protocol encapsulation
    ip4unicast        IPv4 unicast protocol encapsulation
    mep               Define mep id used in OAM based PTP
    oam               OAM encapsulation (only used in Serval based Distributed TC)
    onepps            1PPS master slave synchronization(only used wht Gen2 1588 PHY's)
    onestep           Onestep mode
    oneway            Oneway slave mode (no Delay_req)
    tag               This parameter is ignored, i.e. tagging depends only on the
                      VLAN configuration for the VLAN specified in the VID field
    twostep           Twostep mode
    twoway            Twoway slave mode
    <cr>
(config)# ptp 0 mode slave vid 100
```

Note: A one-step clock updates accurate timestamp (t1) in Sync message; a 2-step clock sends accurate timestamp (t1) in a Follow_Up message.

Messages:
Cannot create clock instance 0 : a P2pTransp clock type already exists
Cannot create clock instance 0 : a BC-frontend clock type already exists

Example:

```
(config)# ptp 0 mode boundary oam
Cannot create clock instance 0 : a P2pTransp clock type already exists
(config)# ptp 0 mode bcfrontend
(config)# ptp 0 mode bcfrontend
Cannot create clock instance 0 : a BC-frontend clock type already exists
(config)#
```

Command: Configure PTP Priority for BMC

Syntax: **ptp** <clockinst> **priority1** <priority1>
ptp <clockinst> **priority2** <priority2>

Description: Configure the clock priority for IEEE 1588 PTP BMC (Best Master Clock) algorithm. The BMC algorithm performs a distributed selection of the best candidate clock based on the several clock properties. The "Priority" is an administratively assigned precedence hint used by the BMC to help select a grandmaster for the PTP domain. IEEE 1588-2002 used a single boolean variable to indicate precedence. IEEE 1588-2008 features two 8-bit priority fields. The parameters are:

priority2 Clock priority 2 for PTP BMC algorithm (0-255; 0 is highest priority).

priority1 Clock priority 1 for PTP BMC algorithm (0-255; 0 is highest priority).

Mode: (config)#

Example 1: Configure PTP instance 0 priority for a BMC:

```
(config)# ptp 0 priority1 ?
    <Priority1 : 0-255>    PTP clock priority1: range = 0-255
(config)# ptp 0 priority1 55 ?
    |       Output modifiers
    <cr>
(config)# ptp 0 priority1 55
(config)# ptp 0 priority2 200
(config)#
(config)# ptp 0 priority1?
    priority1    Clock priority 1 for PTP BMC algorithm (0 is highest priority)
(config)# ptp 0 priority1 ?
    <0-255>    PTP clock priority1: range = 0-255
(config)# ptp 0 priority2?
    priority2    Clock priority 2 for PTP BMC algorithm (0 is highest priority)
(config)# ptp 0 priority2 ?
    <0-255>    PTP clock priority1: range = 0-255
(config)# ptp 0 priority2 100
(config)# ptp 0 priority1 200
(config)#
```

Command: Configure PTP Servo PID

Syntax: **ptp** <clockinst> **servo ad** <ad>
ptp <clockinst> **servo ai** <ai>
ptp <clockinst> **servo ap** <ap>
ptp <clockinst> **servo displaystates**

Description: Configure the IEEE 1588 PTP Servo PID parameters:
<**Ad** : 1-10000> The '**D**' component in the PID servo regulator (1-10000).
<**Ai** : 1-10000> [The '**I**' component in the PID servo regulator (1-10000).
<**Ap** : 1-1000> The '**P**' component in the PID servo regulator (1-10000).

Mode: (config)#

Example 1: Configure PTP instance 0 with valid Servo parameters:

```
(config)# ptp 0 servo ?
    ad               Set 'D' parameter in the servo
    ai               Set 'I' parameter in the servo
    ap               Set 'P' parameter in the servo
    displaystates    Enable logging of servo parameters on the console
(config)# ptp 0 servo ad ?
    <1-10000>    [1..10000] 'D' component in PID servo regulator
(config)# ptp 0 servo ai ?
    <1-10000>    [1..10000] 'I' component in PID servo regulator.
(config)# ptp 0 servo ap ?
    <1-1000>    [1..1000] 'P' component in PID servo regulator
(config)# ptp 0 servo ap 222
(config)# ptp 0 servo ai 650
(config)# ptp 0 servo ad 900
(config)#
```

The default clock servo uses a PID regulator to calculate the current clock rate:

OffsetFromMaster/ P constant
+ Integral(OffsetFromMaster)/ I constant
+ Differential OffsetFromMaster)/ D constant =
clockAdjustment

The Proportional–Integral–Derivative 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 depends on the accumulation of past errors, and
D is a prediction of future errors, based on current rate of change.

Command: Config Logging PTP Servo Display States

Syntax: **ptp** <clockinst> **servo displaystates**

Description: Enable logging of servo parameters on the console.

Mode: (config)#

Example 1: Enable logging of servo parameters on the console:

```
(config)# ptp 0 servo displaystates?
    displaystates    Enable logging of servo parameters on the console
    <cr>
(config)# ptp 0 servo displaystates?
ptp <clockinst> servo displaystates
(config)# ptp 0 servo displaystates
```

Command: Configure PTP Clock Slave

Syntax: **ptp** <clockinst> **slave-cfg** [stable-offset <stable_offset>] [offset-ok <offset_ok>] [offset-fail <offset_fail>]

Description: Set the IEEE 1588 Clock Slave configuration.

StableOffset : Stable offset threshold (0-1000000 ns).

OffsetOk : Offset ok threshold (0-1000000 ns).

OffsetFail : Offset fail threshold (0-1000000 ns).

Mode: (config)#

Example 1: Configure PTP instance 0 slave config:

```
(config)# ptp 0 slave-cfg ?
    offset-fail      set the offset_fail threshold
    offset-ok        set the offset_ok threshold
    stable-offset    set the stable_offset threshold
    <cr>
(config)# ptp 0 slave-cfg?
    slave-cfg    Set PTP clock Slave Configuration
    <cr>
(config)# ptp 0 slave-cfg?
ptp <clockinst> slave-cfg [ stable-offset <stable_offset> ] [ offset-ok <offset_ok> ]
[ offset-fail <offset_fail> ]
(config)# ptp 0 slave-cfg?
    slave-cfg    Set PTP clock Slave Configuration
    <cr>
(config)# ptp 0 slave-cfg offset-fail ?
    <OffsetFail : 0-1000000>    offset_fail threshold in ns
(config)# ptp 0 slave-cfg offset-fail 5000 ?
    offset-ok        set the offset_ok threshold
    stable-offset    set the stable_offset threshold
    <cr>
(config)# ptp 0 slave-cfg offset-fail 5000 offset-ok ?
    <OffsetOk : 0-1000000>    offset_ok threshold in ns
(config)# ptp 0 slave-cfg offset-fail 5000 offset-ok 100000 ?
    stable-offset    set the stable_offset threshold
    <cr>
(config)# $ 0 slave-cfg offset-fail 5000 offset-ok 100000 stable-offset ?
    <StableOffset : 0-1000000>    stable_offset threshold in ns.
(config)# $ 0 slave-cfg offset-fail 5000 offset-ok 100000 stable-offset 99999
(config)#
```

Command: Configure PTP Time Properties

Syntax: **ptp** <clockinst> **time-property** [utc-offset <utc_offset>] [valid] [leap-59 |leap-61] [time-traceable] [freq-traceable] [ptptimescale] [time-source <time_source>]

Description: Configure the IEEE 1588 PTP time property parameters:

freq-traceable frequency is traceable.
leap-59 leap59 in current day.
leap-61 leap61 in current day.
ptptimescale timing is a PTP time scale.
time-source set timesource.
time-traceable timing is traceable.
utc-offset set UTC offset
valid UTC offset is valid.
<cr>

Mode: (config)#

Example 1: Configure PTP instance 0 PTP time property parameters:

```
(config)# ptp 0 time-property freq-traceable?
    freq-traceable    frequency is traceable
    <cr>
(config)# ptp 0 time-property freq-traceable?
(config)# ptp 0 time-property freq-traceable leap-59
(config)# ptp 0 time-property freq-traceable leap-61
(config)# ptp 0 time-property freq-traceable ptptimescale ?
    leap-59           leap59 in current day
    leap-61           leap61 in current day
    time-source       set timesource
    time-traceable    timing is traceable
    utc-offset        set utc offset
    valid             UTC offset is valid
    <cr>
(config)# ptp 0 time-property freq-traceable ptptimescale
(config)# ptp 0 time-property freq-traceable time-source ?
    <TimeSource : 0-255>    timesource: range 0-255
(config)# ptp 0 time-property freq-traceable time-traceable ?
    leap-59         leap59 in current day
    leap-61         leap61 in current day
    ptptimescale    timing is a PTP time scale
    time-source     set timesource
    utc-offset      set utc offset
    valid           UTC offset is valid
    <cr>
(config)# ptp 0 time-property freq-traceable time-traceable
(config)# ptp 0 time-property freq-traceable utc-offset ?
    <UtcOffset : -32768-32767>    utc offset value
(config)# ptp 0 time-property freq-traceable utc-offset 5565
(config)# ptp 0 time-property freq-traceable valid
(config)#
```

Command: Configure PTP Unicast Slave

Syntax: **ptp** <clockinst> **uni** <idx> [duration <duration>] <ip>

Description: Configure the IEEE 1588 PTP Unicast Slave configuration entry.
<**Duration** : 10-1000> The number of seconds for which the Announce/Sync messages are requested (10-1000 seconds).
<**Ip** : ipv4_ucast> The IPv4 address of the requested master clock.

Mode: (config)#

Example 1: Configure PTP instance 0 PTP Unicast Slave duration:

```
(config)# ptp 0 uni 0 ?
    <Ip : ipv4_ucast>    IPv4 address of requested master clock
    duration             Set the Duration parameter
(config)# ptp 0 uni 0 192.168.1.30 ?
    <cr>
(config)# ptp 0 uni 0 192.168.1.30
(config)#
(config)# ptp 0 uni 0 duration ?
    <Duration : 10-1000>    Duration [10..1000]. Number of seconds for which the
                            Announce/Sync messages are requested
(config)# ptp 0 uni 0 duration 200 ?
    <Ip : ipv4_ucast>    IPv4 address of requested master clock
(config)# ptp 0 uni 0 duration 200 192.168.1.30
(config)#
```

Command: Configure PTP External Clock Impedence / Input / Output

Syntax: **ptp ext-clock impedance** { 50 | 75 | hi-z }
ptp ext-clock { { output <output_freq> } | { input <input_freq> } }

Description: Configure the IEEE 1588 PTP External Clock Impedence / Input / Output. An external clock must already exist.

Mode: (config)#

Example 1: Display the varous **ptp ext** command functions.

```
(config)# ptp ext?
ptp ext-clock impedance { 50 | 75 | hi-z }
ptp ext-clock { { output <output_freq> } | { input <input_freq> } }
(config)# ptp ext ?
    impedance    Modify external clock impedance
    input        External input
    output       External output
(config)# ptp ext impedance ?
    50
    75
    hi-z
(config)# ptp ext input ?
    <cword>    Valid words are '1.544mhz' '10mhz' '19.44mhz' '1pps' '2.048mhz'
               '25mhz' '64khz' '8khz'
(config)# ptp ext output ?
    <1-25000000>    External clock output frequency in Hz
(config)# ptp ext output
```

Example 2: Config PTP External Clock Impedence:

```
(config)# ptp ext-clock impedance ?
    50
    75
    hi-z
(config)# ptp ext-clock impedance 75
(config)#
```

Example 3: Config PTP External Clock Input:

```
(config)# ptp ext-clock input ?
    CWORD    Valid words are '1.544mhz' '10mhz' '19.44mhz' '1pps' '2.048mhz'
             '25mhz' '64khz' '8khz'
(config)# ptp ext-clock input 1pps
(config)#
```

Example 4: Config PTP External Clock Output:

```
(config)# ptp ext-clock output ?
    <1-25000000>    External clock output frequency in Hz
(config)# ptp ext-clock output 500000
(config)#
```

Messages:

One_pps_mode overrules clock_out_enable, i.e. clock_out_enable is set to false

External Clock feature not present

Command: Config PTP Internal TC Mode

Syntax: **ptp tc-internal** [**mode** <mode>]

Description: Configure the IEEE 1588 PTP TC (Transparent Clock) internal mode (0-3). Note that you must re-boot the S4224 when changing the internal mode. The parameters are:

0 = 30 Bit Mode.
1 = 32 Bit Mode.
2 = 44 Bit Mode.
3 = 48 Bit Mode.

Mode: (config)

Example 1: Configure PTP instance 0 Transparent Clock internal mode:

```
(config)# ptp tc-internal mode ?
    <Mode : 0-8>    mode [0-3] (0 = MODE_30BIT, 1 = MODE_32BIT, 2 = MODE_44BIT,
                    3 = MODE_48BIT)
(config)# ptp tc-internal mode?
    mode    Set mode
(config)# ptp tc-internal mode?
ptp tc-internal [ mode <mode> ]
(config)# ptp tc-internal mode 0 ?
    <cr>
(config)# ptp tc-internal mode 0

Successfully set the TC internal mode...
Internal TC mode Configuration has been set, you need to reboot to activate the
changed conf.
(config)# ptp tc-internal mode 1

Successfully set the TC internal mode...
Internal TC mode Configuration has been set, you need to reboot to activate the
changed conf.
(config)# ptp tc-internal mode 2

Successfully set the TC internal mode...
Internal TC mode Configuration has been set, you need to reboot to activate the
changed conf.
(config)#
```

Command: Configure QoS

Syntax: **config qos**

Description: Configure QoS (Quality of Service) in terms of map, QCE, storm, and WRED parameters.

Mode: (config)#

Example: Display the various **qos** command functions:

```
(config)# qos?
    qos    Quality of Service
(config)# qos ?
    map      Global QoS Map/Table
    qce      QoS Control Entry
    wred     Weighted Random Early Discard
(config)# qos??
    qos    Quality of Service
(config)# qos??
qos map cos-dscp <cos> dpl <dpl> dscp { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23
| af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3| cs4 | cs5 | cs6 | cs7 | ef | va } }
qos map dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 |
af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }qos map dscp-cos {
<dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 |
af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } cos <cos> dpl <dpl>
qos map dscp-egress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21| af22 | af23 | af31
| af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4| cs5 | cs6 | cs7 | ef | va } } <dpl> to {
<dscp_num_tr> | { be | af11 | af12 |af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 |
af43 | cs1 | cs2| cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }qos map dscp-ingress-translation {
<dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 |
af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } to { <dscp_num_tr> | { be | af11 | af12
| af13| af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 |
cs6 | cs7 | ef | va } } qos qce refresh qos qce { [ update ] } <qce_id> [ { next <qce_id_next> } |
last ] [ interface (<port_type> [ <port_list> ] ) ] [ smac { <smac> | <smac_24> | any } ] [ dmac { <
dmac> | unicast | multicast | broadcast | any } ] [ tag { [ type { untagged | tagged | c-tagged | s-
tagged | any } ] [ vid { <ot_vid> | any } ] [ pcp { <ot_pcp> | any } ] [ dei { <ot_dei> | any } ]
}*1 ] [ inner-tag { [ type { untagged | tagged | c-tagged | s-tagged | any } ] [ vid { <it_vid> |
any } ] [ pcp { <it_pcp> | any } ] [ dei { <it_dei> | any } ] }*1 ] [ frame-type { any | { etype [ {
<etype_type> | any } ] } | { llc [ dsap { <llc_dsap> | any } ] [ ssap { <llc_ssap>| any } ] [
control { <llc_control> | any } ] } | { snap [ { <snap_data> | any } ] } | { ipv4 [ proto { <pr4> |
tcp | udp | any } ] [ sip { <sip4> | any } ] [ dip { <dip4> | any } ] [ dscp { <dscp4> | { be | af11
| af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4
| cs5 | cs6 | cs7 | ef | va } | any } ] [ fragment { yes | no | any } ] [ sport { <sp4> | any } ] [
dport { <dp4> | any } ] } | { ipv6 [ proto { <pr6> | tcp | udp | any } ] [ sip { <sip6> | any } ] [
dip { <dip6> | any } ] [ dscp { <dscp6> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 |
af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any } ] [
sport { <sp6> | any } ] [ dport { <dp6> | any } ] } } ] [ action { [ cos { <action_cos> | default }
] [ dpl { <action_dpl> | default } ] [ pcp-dei { <action_pcp> <action_dei> | default } ] [ dscp {
<action_dscp_dscp> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 |
af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | default } ] [ policy {
<action_policy> | default } ] }*1 ] qos wred queue <queue> min-th <min_th> mdp-1 <mdp_1> mdp-2
<mdp_2> mdp-3 <mdp_3
(config)# qos
```

Command: Configure Global QoS Map/Table

Syntax: **config qos map**

Description: Configure QoS (Quality of Service) Global QoS Map/Table parameters.

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

Mode: (config)

Example 1: Display the various **qos map cos-dscp** command functions:

```
(config)# qos map cos-dscp?
    cos-dscp    Map for cos to dscp
(config)# qos map cos-dscp?
qos map cos-dscp <cos> dpl <dpl> dscp { <dscp_num> | { be | af11 | af12 | af13 |
 af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3
| cs4 | cs5 | cs6 | cs7 | ef | va } }
(config)# qos map cos-dscp?
    cos-dscp    Map for cos to dscp
(config)# qos map cos-dscp 3 dpl 0 dscp ?
    <0-63>    Specific DSCP
    af11      Assured Forwarding PHB AF11(DSCP 10)
    af12      Assured Forwarding PHB AF12(DSCP 12)
    af13      Assured Forwarding PHB AF13(DSCP 14)
    af21      Assured Forwarding PHB AF21(DSCP 18)
    af22      Assured Forwarding PHB AF22(DSCP 20)
    af23      Assured Forwarding PHB AF23(DSCP 22)
    af31      Assured Forwarding PHB AF31(DSCP 26)
    af32      Assured Forwarding PHB AF32(DSCP 28)
    af33      Assured Forwarding PHB AF33(DSCP 30)
    af41      Assured Forwarding PHB AF41(DSCP 34)
    af42      Assured Forwarding PHB AF42(DSCP 36)
    af43      Assured Forwarding PHB AF43(DSCP 38)
    be        Default PHB(DSCP 0) for best effort traffic
    cs1       Class Selector PHB CS1 precedence 1(DSCP 8)
    cs2       Class Selector PHB CS2 precedence 2(DSCP 16)
    cs3       Class Selector PHB CS3 precedence 3(DSCP 24)
    cs4       Class Selector PHB CS4 precedence 4(DSCP 32)
    cs5       Class Selector PHB CS5 precedence 5(DSCP 40)
    cs6       Class Selector PHB CS6 precedence 6(DSCP 48)
    cs7       Class Selector PHB CS7 precedence 7(DSCP 56)
    ef        Expedited Forwarding PHB(DSCP 46)
    va        Voice Admit PHB(DSCP 44)
(config)# qos map cos-dscp 3 dpl 0 dscp be ?
    <cr>
(config)# qos map cos-dscp 3 dpl 0 dscp be
(config)# qos map cos-dscp?
    cos-dscp    Map for cos to dscp
(config)# qos map cos-dscp
```

Example 2: qos map dscp-classify

```
(config)# qos map cos-dscp?
    cos-dscp    Map for cos to dscp
(config)# qos map dscp-classify?
    dscp-classify    Map for dscp classify enable
(config)# qos map dscp-classify ?
    <0~63>    Specific DSCP or range
    af11      Assured Forwarding PHB AF11(DSCP 10)
    af12      Assured Forwarding PHB AF12(DSCP 12)
    af13      Assured Forwarding PHB AF13(DSCP 14)
    af21      Assured Forwarding PHB AF21(DSCP 18)
    af22      Assured Forwarding PHB AF22(DSCP 20)
    af23      Assured Forwarding PHB AF23(DSCP 22)
    af31      Assured Forwarding PHB AF31(DSCP 26)
    af32      Assured Forwarding PHB AF32(DSCP 28)
    af33      Assured Forwarding PHB AF33(DSCP 30)
    af41      Assured Forwarding PHB AF41(DSCP 34)
    af42      Assured Forwarding PHB AF42(DSCP 36)
    af43      Assured Forwarding PHB AF43(DSCP 38)
    be        Default PHB(DSCP 0) for best effort traffic
    cs1       Class Selector PHB CS1 precedence 1(DSCP 8)
    cs2       Class Selector PHB CS2 precedence 2(DSCP 16)
    cs3       Class Selector PHB CS3 precedence 3(DSCP 24)
    cs4       Class Selector PHB CS4 precedence 4(DSCP 32)
    cs5       Class Selector PHB CS5 precedence 5(DSCP 40)
    cs6       Class Selector PHB CS6 precedence 6(DSCP 48)
    cs7       Class Selector PHB CS7 precedence 7(DSCP 56)
    ef        Expedited Forwarding PHB(DSCP 46)
    va        Voice Admit PHB(DSCP 44)
(config)# qos map dscp-classify be ?
    <cr>
(config)# qos map dscp-classify be
(config)#
```

Example 3: qos map dscp-cos

```
(config)# qos map dscp-cos ?
    <DscpNum : 0~63>    Specific DSCP or range
    af11                Assured Forwarding PHB AF11(DSCP 10)
    af12                Assured Forwarding PHB AF12(DSCP 12)
    af13                Assured Forwarding PHB AF13(DSCP 14)
    af21                Assured Forwarding PHB AF21(DSCP 18)
    af22                Assured Forwarding PHB AF22(DSCP 20)
    af23                Assured Forwarding PHB AF23(DSCP 22)
    af31                Assured Forwarding PHB AF31(DSCP 26)
    af32                Assured Forwarding PHB AF32(DSCP 28)
    af33                Assured Forwarding PHB AF33(DSCP 30)
    af41                Assured Forwarding PHB AF41(DSCP 34)
    af42                Assured Forwarding PHB AF42(DSCP 36)
    af43                Assured Forwarding PHB AF43(DSCP 38)
    be                  Default PHB(DSCP 0) for best effort traffic
    cs1                 Class Selector PHB CS1 precedence 1(DSCP 8)
    cs2                 Class Selector PHB CS2 precedence 2(DSCP 16)
    cs3                 Class Selector PHB CS3 precedence 3(DSCP 24)
    cs4                 Class Selector PHB CS4 precedence 4(DSCP 32)
    cs5                 Class Selector PHB CS5 precedence 5(DSCP 40)
    cs6                 Class Selector PHB CS6 precedence 6(DSCP 48)
    cs7                 Class Selector PHB CS7 precedence 7(DSCP 56)
    ef                  Expedited Forwarding PHB(DSCP 46)
    va                  Voice Admit PHB(DSCP 44)
(config)# qos map dscp-cos af11 ?
    cos    Specify class of service
```

```
(config)# qos map dscp-cos af11 cos ?
    <Cos : 0-7>    Specific class of service
(config)# qos map dscp-cos af11 cos 5 ?
    dpl    Specify drop precedence level
(config)# qos map dscp-cos af11 cos 5 dpl ?
    <Dpl : dpl>    Specific drop precedence level
(config)# qos map dscp-cos af11 cos 5 dpl 0 ?
    <cr>
(config)# qos map dscp-cos af11 cos 5 dpl 0
(config)#
```

Example 4: dscp-egress-translation

```
qos map dscp-egress-translation
(config)# qos map dscp-egress-translation ?
    <DscpNum : 0~63>    Specific DSCP or range
    af11                Assured Forwarding PHB AF11(DSCP 10)
    af12                Assured Forwarding PHB AF12(DSCP 12)
    af13                Assured Forwarding PHB AF13(DSCP 14)
    af21                Assured Forwarding PHB AF21(DSCP 18)
    af22                Assured Forwarding PHB AF22(DSCP 20)
    af23                Assured Forwarding PHB AF23(DSCP 22)
    af31                Assured Forwarding PHB AF31(DSCP 26)
    af32                Assured Forwarding PHB AF32(DSCP 28)
    af33                Assured Forwarding PHB AF33(DSCP 30)
    af41                Assured Forwarding PHB AF41(DSCP 34)
    af42                Assured Forwarding PHB AF42(DSCP 36)
    af43                Assured Forwarding PHB AF43(DSCP 38)
    be                  Default PHB(DSCP 0) for best effort traffic
    cs1                 Class Selector PHB CS1 precedence 1(DSCP 8)
    cs2                 Class Selector PHB CS2 precedence 2(DSCP 16)
    cs3                 Class Selector PHB CS3 precedence 3(DSCP 24)
    cs4                 Class Selector PHB CS4 precedence 4(DSCP 32)
    cs5                 Class Selector PHB CS5 precedence 5(DSCP 40)
    cs6                 Class Selector PHB CS6 precedence 6(DSCP 48)
    cs7                 Class Selector PHB CS7 precedence 7(DSCP 56)
    ef                  Expedited Forwarding PHB(DSCP 46)
    va                  Voice Admit PHB(DSCP 44)
(config)# qos map dscp-egress-translation cs1 ?
    <Dpl : 0~1>    Specific drop precedence level or range
(config)# qos map dscp-egress-translation cs1 1 to ?
    <DscpNumTr : 0-63>    Translated DSCP value
    af11                  Assured Forwarding PHB AF11(DSCP 10)
    af12                  Assured Forwarding PHB AF12(DSCP 12)
    af13                  Assured Forwarding PHB AF13(DSCP 14)
    af21                  Assured Forwarding PHB AF21(DSCP 18)
    af22                  Assured Forwarding PHB AF22(DSCP 20)
    af23                  Assured Forwarding PHB AF23(DSCP 22)
    af31                  Assured Forwarding PHB AF31(DSCP 26)
    af32                  Assured Forwarding PHB AF32(DSCP 28)
    af33                  Assured Forwarding PHB AF33(DSCP 30)
    af41                  Assured Forwarding PHB AF41(DSCP 34)
    af42                  Assured Forwarding PHB AF42(DSCP 36)
    af43                  Assured Forwarding PHB AF43(DSCP 38)
    be                    Default PHB(DSCP 0) for best effort traffic
    cs1                   Class Selector PHB CS1 precedence 1(DSCP 8)
    cs2                   Class Selector PHB CS2 precedence 2(DSCP 16)
    cs3                   Class Selector PHB CS3 precedence 3(DSCP 24)
    cs4                   Class Selector PHB CS4 precedence 4(DSCP 32)
    cs5                   Class Selector PHB CS5 precedence 5(DSCP 40)
    cs6                   Class Selector PHB CS6 precedence 6(DSCP 48)
    cs7                   Class Selector PHB CS7 precedence 7(DSCP 56)
```

```
    ef                    Expedited Forwarding PHB(DSCP 46)
    va                    Voice Admit PHB(DSCP 44)
(config)# qos map dscp-egress-translation cs1 1 to af11 ?
    <cr>
(config)# qos map dscp-egress-translation cs1 1 to af11
(config)#
```

Example 5: qos map dscp-ingress-translation

```
 (config)# qos map dscp-ingress-translation ?
    <DscpNum : 0~63>    Specific DSCP or range
    af11                Assured Forwarding PHB AF11(DSCP 10)
    af12                Assured Forwarding PHB AF12(DSCP 12)
    af13                Assured Forwarding PHB AF13(DSCP 14)
    af21                Assured Forwarding PHB AF21(DSCP 18)
    af22                Assured Forwarding PHB AF22(DSCP 20)
    af23                Assured Forwarding PHB AF23(DSCP 22)
    af31                Assured Forwarding PHB AF31(DSCP 26)
    af32                Assured Forwarding PHB AF32(DSCP 28)
    af33                Assured Forwarding PHB AF33(DSCP 30)
    af41                Assured Forwarding PHB AF41(DSCP 34)
    af42                Assured Forwarding PHB AF42(DSCP 36)
    af43                Assured Forwarding PHB AF43(DSCP 38)
    be                  Default PHB(DSCP 0) for best effort traffic
    cs1                 Class Selector PHB CS1 precedence 1(DSCP 8)
    cs2                 Class Selector PHB CS2 precedence 2(DSCP 16)
    cs3                 Class Selector PHB CS3 precedence 3(DSCP 24)
    cs4                 Class Selector PHB CS4 precedence 4(DSCP 32)
    cs5                 Class Selector PHB CS5 precedence 5(DSCP 40)
    cs6                 Class Selector PHB CS6 precedence 6(DSCP 48)
    cs7                 Class Selector PHB CS7 precedence 7(DSCP 56)
    ef                  Expedited Forwarding PHB(DSCP 46)
    va                  Voice Admit PHB(DSCP 44)
(config)# qos map dscp-ingress-translation 45 to ?
    <DscpNumTr : 0-63>    Translated DSCP value
    af11                  Assured Forwarding PHB AF11(DSCP 10)
    af12                  Assured Forwarding PHB AF12(DSCP 12)
    af13                  Assured Forwarding PHB AF13(DSCP 14)
    af21                  Assured Forwarding PHB AF21(DSCP 18)
    af22                  Assured Forwarding PHB AF22(DSCP 20)
    af23                  Assured Forwarding PHB AF23(DSCP 22)
    af31                  Assured Forwarding PHB AF31(DSCP 26)
    af32                  Assured Forwarding PHB AF32(DSCP 28)
    af33                  Assured Forwarding PHB AF33(DSCP 30)
    af41                  Assured Forwarding PHB AF41(DSCP 34)
    af42                  Assured Forwarding PHB AF42(DSCP 36)
    af43                  Assured Forwarding PHB AF43(DSCP 38)
    be                    Default PHB(DSCP 0) for best effort traffic
    cs1                   Class Selector PHB CS1 precedence 1(DSCP 8)
    cs2                   Class Selector PHB CS2 precedence 2(DSCP 16)
    cs3                   Class Selector PHB CS3 precedence 3(DSCP 24)
    cs4                   Class Selector PHB CS4 precedence 4(DSCP 32)
    cs5                   Class Selector PHB CS5 precedence 5(DSCP 40)
    cs6                   Class Selector PHB CS6 precedence 6(DSCP 48)
    cs7                   Class Selector PHB CS7 precedence 7(DSCP 56)
    ef                    Expedited Forwarding PHB(DSCP 46)
    va                    Voice Admit PHB(DSCP 44)
(config)# qos map dscp-ingress-translation 45 to cs5 ?
    <cr>
(config)# qos map dscp-ingress-translation 45 to cs5
(config)#
```

Command: Configure QoS QCE

Syntax: **qos qce**

Description: Configure QoS (Quality of Service) QCE (QoS Control Entry). Note that at least one action parameter must have a non-default value. The QCL (QoS Control List configuration is a table of QCEs, containing QoS control entries that classify to a Specific QoS class on specific traffic objects. A QoS class is associated with a particular QCE ID. There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of four different QoS classes ("Low", "Normal", "Medium", and "High)" for individual application.The parameters are:

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

Mode: (config)#

Example 1: qos qce 1

```
(config)# qos qce 1 ?
    action        Setup action
    dmac          Setup matched DMAC
    frame-type    Setup matched frame type
    interface     Interfaces
    last          Place QCE at the end
    next          Place QCE before the next QCE ID
    smac          Setup matched SMAC
    tag           Setup tag options
    <cr>
(config)# qos qce refresh ?
    <cr>
(config)# qos qce update ?
    <Id : 1-256>    QCE ID
(config)# qos qce update
```

Example 2: qos qce 1 action

```
(config)# qos qce 1 action ?
    cos     Setup class of service action
    dpl     Setup drop precedence level action
    dscp    Setup DSCP action
    pcp-dei    Setup PCP and DEI action
    policy     Setup ACL policy action
(config)# qos qce 1 action cos ?
    <Cos : 0-7>    Assign class of service
    default        Keep existing class of service
(config)# qos qce 1 action cos 1 ?
    dmac          Setup matched DMAC
    dpl           Setup drop precedence level action
    dscp          Setup DSCP action
    frame-type    Setup matched frame type
    inner-tag     Setup inner tag options
    interface     Interfaces
    last          Place QCE at the end
    next          Place QCE before the next QCE ID
    pcp-dei       Setup PCP and DEI action
    policy        Setup ACL policy action
    smac          Setup matched SMAC
    tag           Setup tag options
    <cr>
```

```
(config)# qos qce 1 action cos 1 dmac ?
    any          Match any DMAC
    broadcast    Match broadcast DMAC
    multicast    Match multicast DMAC
    unicast      Match unicast DMAC
(config)# qos qce 1 action cos 1 dmac unicast ?
    frame-type    Setup matched frame type
    inner-tag     Setup inner tag options
    interface     Interfaces
    last          Place QCE at the end
    next          Place QCE before the next QCE ID
    smac          Setup matched SMAC
    tag           Setup tag options
    <cr>
(config)# qos qce 1 action cos 1 dmac unicast frame-type ?
    any      Match any frame type
    etype    Match EtherType frames
    ipv4     Match IPv4 frames
    ipv6     Match IPv6 frames
    llc      Match LLC frames
    snap     Match SNAP frames
(config)# qos qce 1 action cos 1 dmac unicast frame-type ipv4 ?
    dip          Setup matched destination IP address
    dport        Setup matched UDP/TCP destination port
    dscp         Setup matched DSCP
    fragment     Setup matched IPv4 fragments
    inner-tag    Setup inner tag options
    interface    Interfaces
    last         Place QCE at the end
    next         Place QCE before the next QCE ID
    proto        Setup matched IP protocol
    sip          Setup matched source IP address
    smac         Setup matched SMAC
    sport        Setup matched UDP/TCP source port
    tag          Setup tag options
    <cr>
(config)# qos qce 1 action cos 1 dmac unicast frame-type ipv4 dport ?
    <vcap_vr>    Match UDP/TCP destination port value/range
    any          Match any UDP/TCP destination port
(config)# qos qce 1 action cos 1 dmac unicast frame-type ipv4 dport any ?
    dip          Setup matched destination IP address
    dscp         Setup matched DSCP
    fragment     Setup matched IPv4 fragments
    inner-tag    Setup inner tag options
    interface    Interfaces
    last         Place QCE at the end
    next         Place QCE before the next QCE ID
    proto        Setup matched IP protocol
    sip          Setup matched source IP address. If 'qos qce addr destination'
                 is set, this parameter specifies the destination IP
    smac         Setup matched SMAC. If 'qos qce addr destination' is set, this
                 parameter specifies the DMAC
    sport        Setup matched UDP/TCP source port
    tag          Setup tag options
    <cr>
```

```
(config)# $ction cos 1 dmac unicast frame-type ipv4 dport any interface ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
(config)# $ unicast frame-type ipv4 dport any interface GigabitEthernet ?
    PORT_LIST    Port list in 1/1-6
(config)# $ unicast frame-type ipv4 dport any interface GigabitEthernet 1/1 ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
    last                Place QCE at the end
    next                Place QCE before the next QCE ID
    smac                Setup matched SMAC
    tag                 Setup tag options
    <cr>
(config)# $rame-type ipv4 dport any interface GigabitEthernet 1/1 last ?
    smac    Setup matched SMAC. If 'qos qce addr destination' is set, this
            parameter specifies the DMAC
    tag     Setup tag options
    <cr>
(config)# $-type ipv4 dport any interface GigabitEthernet 1/1 last smac ?
    <Smac : mac_addr>   Matched SMAC (XX-XX-XX-XX-XX-XX)
    any                 Match any SMAC
(config)# $-type ipv4 dport any interface GigabitEthernet 1/1 last smac any ?
    tag     Setup tag options
    <cr>
(config)# $v4 dport any interface GigabitEthernet 1/1 last smac any tag ?
    dei     Setup matched DEI
    pcp     Setup matched PCP
    type    Setup matched tag type
    vid     Setup matched VLAN ID
(config)# $v4 dport any interface GigabitEthernet 1/1 last smac any tag vid ?
    <Vid : 0-4095>    Matched VLAN ID value/range
    any               Match any VLAN ID
(config)# $ny interface GigabitEthernet 1/1 last smac any tag vid 1 ?
    dei     Setup matched DEI
    pcp     Setup matched PCP
    type    Setup matched tag type
    <cr>
(config)# $ny interface GigabitEthernet 1/1 last smac any tag vid 1
(config)# $y interface GigabitEthernet 1/1 last smac any tag vid 1 dei ?
    <Dei : 0-1>    Matched DEI
    any            Match any DEI
(config)# $y interface GigabitEthernet 1/1 last smac any tag vid 1 dei 0 ?
    pcp     Setup matched PCP
    type    Setup matched tag type
    <cr>
(config)# $erface GigabitEthernet 1/1 last smac any tag vid 1 dei 0 pcp ?
    <Pcp : pcp>    Matched PCP value/range
    any            Match any PCP
(config)# $erface GigabitEthernet 1/1 last smac any tag vid 1 dei 0 pcp 1 ?
    type    Setup matched tag type
    <cr>
(config)# $GigabitEthernet 1/1 last smac any tag vid 1 dei 0 pcp 1 type ?
    any         Match tagged and untagged frames
    tagged      Match tagged frames
    untagged    Match untagged frames
(config)# $GigabitEthernet 1/1 last smac any tag vid 1 dei 0 pcp 1 type any
(config)#
```

Example 3: qos qce 1 dmac

```
(config)# qos qce 1 dmac ?
    any           Match any DMAC
    broadcast     Match broadcast DMAC
    multicast     Match multicast DMAC
    unicast       Match unicast DMAC
(config)# qos qce 1 dmac broadcast ?
    action        Setup action
    frame-type    Setup matched frame type
    inner-tag     Setup inner tag options
    interface     Interfaces
    last          Place QCE at the end
    next          Place QCE before the next QCE ID
    smac          Setup matched SMAC.
    tag           Setup tag options
    <cr>
(config)# qos qce 1 dmac broadcast action ?
    cos        Setup class of service action
    dpl        Setup drop precedence level action
    dscp       Setup DSCP action
    pcp-dei    Setup PCP and DEI action
    policy     Setup ACL policy action
(config)# qos qce 1 dmac broadcast action dscp ?
    <0-63>     Assign DSCP
    af11       Assured Forwarding PHB AF11(DSCP 10)
    af12       Assured Forwarding PHB AF12(DSCP 12)
    af13       Assured Forwarding PHB AF13(DSCP 14)
    af21       Assured Forwarding PHB AF21(DSCP 18)
    af22       Assured Forwarding PHB AF22(DSCP 20)
    af23       Assured Forwarding PHB AF23(DSCP 22)
    af31       Assured Forwarding PHB AF31(DSCP 26)
    af32       Assured Forwarding PHB AF32(DSCP 28)
    af33       Assured Forwarding PHB AF33(DSCP 30)
    af41       Assured Forwarding PHB AF41(DSCP 34)
    af42       Assured Forwarding PHB AF42(DSCP 36)
    af43       Assured Forwarding PHB AF43(DSCP 38)
    be         Default PHB(DSCP 0) for best effort traffic
    cs1        Class Selector PHB CS1 precedence 1(DSCP 8)
    cs2        Class Selector PHB CS2 precedence 2(DSCP 16)
    cs3        Class Selector PHB CS3 precedence 3(DSCP 24)
    cs4        Class Selector PHB CS4 precedence 4(DSCP 32)
    cs5        Class Selector PHB CS5 precedence 5(DSCP 40)
    cs6        Class Selector PHB CS6 precedence 6(DSCP 48)
    cs7        Class Selector PHB CS7 precedence 7(DSCP 56)
    default    Keep existing DSCP
    ef         Expedited Forwarding PHB(DSCP 46)
    va         Voice Admit PHB(DSCP 44)
(config)# qos qce 1 dmac broadcast action dscp be ?
    cos           Setup class of service action
    dpl           Setup drop precedence level action
    frame-type    Setup matched frame type
    inner-tag     Setup inner tag options
    interface     Interfaces
    last          Place QCE at the end
    next          Place QCE before the next QCE ID
    pcp-dei       Setup PCP and DEI action
    policy        Setup ACL policy action
    smac          Setup matched SMAC
    tag           Setup tag options
    <cr>
(config)# qos qce 1 dmac broadcast action dscp be
(config)#
```

Example 4: qos qce 1 frame-type

```
(config)# qos qce 1 frame-type ?
    any      Match any frame type
    etype    Match EtherType frames
    ipv4     Match IPv4 frames
    ipv6     Match IPv6 frames
    llc      Match LLC frames
    snap     Match SNAP frames
(config)# qos qce 1 frame-type etype ?
    <EtherType : 0x600-0x7ff,0x801-0x86dc,0x86de-0xffff>    Matched EtherType
    action                                                  Setup action
    any                                                     Match any EtherType
    dmac                                                    Setup matched DMAC
    inner-tag                                               Setup inner tag
                                                            options
    interface                                               Interfaces
    last                                                    Place QCE at the
                                                            end
    next                                                    Place QCE before
                                                            the next QCE ID
    smac                                                    Setup matched SMAC
    tag                                                     Setup tag options
    <cr>
(config)# qos qce 1 frame-type etype tag ?
    dei     Setup matched DEI
    pcp     Setup matched PCP
    type    Setup matched tag type
    vid     Setup matched VLAN ID
(config)# qos qce 1 frame-type etype tag type ?
    any         Match tagged and untagged frames
    c-tagged    Match C-tagged frames
    s-tagged    Match S-tagged frames
    tagged      Match tagged frames
    untagged    Match untagged frames
(config)# qos qce 1 frame-type etype tag type any ?
    action       Setup action
    dei          Setup matched DEI
    dmac         Setup matched DMAC
    inner-tag    Setup inner tag options
    interface    Interfaces
    last         Place QCE at the end
    next         Place QCE before the next QCE ID
    pcp          Setup matched PCP
    smac         Setup matched SMAC. If 'qos qce addr destination' is set, this
                 parameter specifies the DMAC
    vid          Setup matched VLAN ID
    <cr>
(config)# qos qce 1 frame-type etype tag type any action ?
    cos     Setup class of service action
    dpl     Setup drop precedence level action
    dscp    Setup DSCP action
    pcp-dei    Setup PCP and DEI action
    policy     Setup ACL policy action
(config)# qos qce 1 frame-type etype tag type any action cos ?
    <Cos : 0-7>    Assign class of service
    default        Keep existing class of service
(config)# qos qce 1 frame-type etype tag type any action cos default ?
    dmac         Setup matched DMAC
    dpl          Setup drop precedence level action
    dscp         Setup DSCP action
    inner-tag    Setup inner tag options
```

```
    interface    Interfaces
    last         Place QCE at the end
    next         Place QCE before the next QCE ID
    pcp-dei      Setup PCP and DEI action
    policy       Setup ACL policy action
    smac         Setup matched SMAC.
    <cr>
(config)# qos qce 1 frame-type etype tag type any action cos default d?
    dmac    Setup matched DMAC
    dpl     Setup drop precedence level action
    dscp    Setup DSCP action
    <cr>
(config)# qos qce 1 frame-type etype tag type any action cos default dmac ?
    <Dmac : mac_addr>    Matched DMAC (XX-XX-XX-XX-XX-XX)
    any                  Match any DMAC
    broadcast            Match broadcast DMAC
    multicast            Match multicast DMAC
    unicast              Match unicast DMAC
(config)# $me-type etype tag type any action cos default dmac multicast ?
    inner-tag    Setup inner tag options
    interface    Interfaces
    last         Place QCE at the end
    next         Place QCE before the next QCE ID
    smac         Setup matched SMAC
    <cr>
(config)# $ype tag type any action cos default dmac multicast interface ?
    *                     All switches or All ports
    GigabitEthernet       1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
(config)# $tion cos default dmac multicast interface 10GigabitEthernet ?
    PORT_LIST    Port list in 1/1-2
(config)# $tion cos default dmac multicast interface 10GigabitEthernet 1/3
% No such port: 10GigabitEthernet 1/3

(config)# $ default dmac multicast interface 10GigabitEthernet 1/1
%QOS: at least one action parameter must have a non-default value
(config)#
```

Command: QoS QCE Refresh

Syntax: **qos qce refresh**
Description: Refresh the QCE tables in S4224 hardware.
Mode: (config)#
Example: Refresh the S4224 QCE tables:

```
(config)# qos qce r?
    refresh    Refresh QCE tables in hardware
    <cr>
(config)# qos qce refresh ?
    <cr>
```

Command: QoS QCE Update

Syntax: **qos qce update** <Id : 1-1024>
Description: Update an existing QCE. The parameters are the same as for creating a QoS QCE.
Mode: (config)#
Example: Update an existing QCE's parameters:

```
(config)# qos qce update ?
    <1-256>    QCE ID
(config)# qos qce update 1 ?
    action        Setup action
    dmac          Setup matched DMAC
    frame-type    Setup matched frame type
    interface     Interfaces
    last          Place QCE at the end
    next          Place QCE before the next QCE ID
    smac          Setup matched SMAC
    tag           Setup tag options
    <cr>
(config)# qos qce update 1 action ?
    cos        Setup class of service action
    dpl        Setup drop precedence level action
    dscp       Setup DSCP action
(config)# qos qce update 1 dmac ?
    any          Match any DMAC
    broadcast    Match broadcast DMAC
    multicast    Match multicast DMAC
    unicast      Match unicast DMAC
(config)# qos qce update 1 frame-type ?
    any      Match any frame type
    etype    Match EtherType frames
    ipv4     Match IPv4 frames
    ipv6     Match IPv6 frames
    llc      Match LLC frames
    snap     Match SNAP frames
```

```
(config)# qos qce update 1 interface ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
(config)# qos qce update 1 last ?
    action        Setup action
    dmac          Setup matched DMAC
    frame-type    Setup matched frame type
    interface     Interfaces
    smac          Setup matched SMAC
    tag           Setup tag options
    <cr>
(config)# qos qce update 1 next ?
    <1-256>    The next QCE ID
(config)# qos qce update 1 next
(config)# qos qce update 1 smac ?
    <oui>    Matched SMAC OUI (XX-XX-XX)
    any      Match any SMAC
(config)# qos qce update 1 tag ?
    dei     Setup matched DEI
    pcp     Setup matched PCP
    type    Setup matched tag type
    vid     Setup matched VLAN ID
(config)# qos qce update 1 tag
```

Command: Configure QoS Storm Policer

Syntax: **qos storm** { unicast | multicast | broadcast } { { <rate> [kfps] } | { 1024 kfps } }

Description: Configure QoS (Quality of Service) parameters.
broadcast Police broadcast frames
multicast Police multicast frames
unicast Police unicast frames

Mode: (config)#

Example: Display the configurable parameters and configure QoS:

```
(config)# qos ?
    map      Global QoS Map/Table
    qce      QoS Control Entry
    wred     Weighted Random Early Discard
(config)# qos storm ?
    broadcast    Police broadcast frames
    multicast    Police multicast frames
    unicast      Police unicast frames
(config)# qos storm broadcast ?
    <1-1024000>    Policer rate (default fps). Internally rounded up to the
                   nearest value supported by the storm policer.
(config)# qos storm multicast ?
    <1-1024000>    Policer rate (default fps). Internally rounded up to the
                   nearest value supported by the storm policer.
(config)# qos storm unicast ?
    <1-1024000>    Policer rate (default fps). Internally rounded up to the
                   nearest value supported by the storm policer.
(config)# qos storm unicast 50000 ?
    fps     Unit is frames per second (default)
    kfps    Unit is kiloframes per second
    <cr>
(config)# qos storm unicast 50000 kfps
% QOS: max rate is 1024 when using kfps
(config)# qos storm unicast 50000 fps
(config)# qos storm multicast 50000
(config)# qos storm multicast 50000 fps
(config)# qos storm broadcast 50000 fps
(config)#
```

The QOS maximum rate is **1024** when using **kfps**.

Command: Configure QoS WRED Queue

Syntax: **qos wred queue** <queue> min-th <min_th> mdp-1 <mdp_1> mdp-2 <mdp_2> mdp-3 <mdp_3

Description: Configure QoS (Quality of Service) in terms of WRED parameters. You can configure the Random Early Detection (RED) settings for queues 0 to 5. RED cannot be applied to queue 6 and 7. Through different RED configuration for the queues (QoS classes) it is possible to obtain Weighted Random Early Detection (WRED) operation between queues. The settings are global for all S4224 ports.
queue : Queue instance (0-5). The queue number (QoS class) that the configuration below applies to.
min-th : Specify minimum threshold in percent <0-100>. If the average queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100.
mdp-1 : Specify drop probability for DPL 1 in percent <0-100>.
mdp-2 : Specify drop probability for DPL 2 in percent <0-100>.
mdp-3 : Specify drop probability for DPL 3 in percent <0-100>.

Mode: (config)#

Example: Change the QoS WRED configuration and show the resulting config:

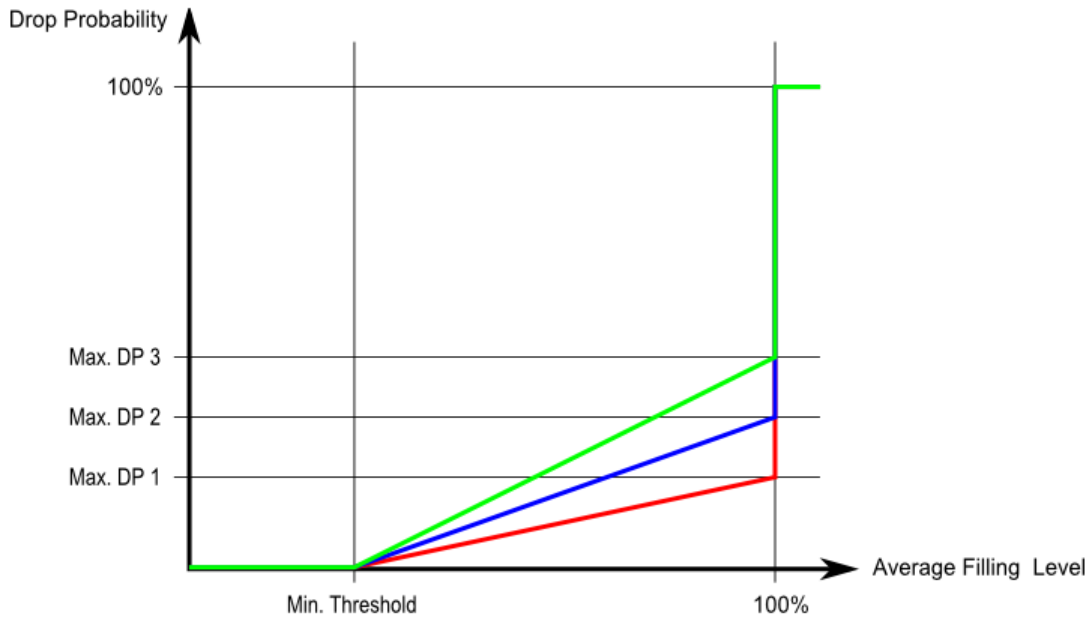
```
(config)# qos wred queue ?
    0~5    Specific queue or range
(config)# qos wred queue 0 ?
    min-th    Specify minimum threshold
(config)# qos wred queue 0 min-th ?
    <0-100>    Specific minimum threshold in percent
(config)# qos wred queue 0 min-th 20 ?
    mdp-1    Specify drop probability for drop precedence level 1
(config)# qos wred queue 0 min-th 20 mdp-1 ?
    <0-100>    Specific drop probability in percent
(config)# qos wred queue 0 min-th 20 mdp-1 30 ?
    mdp-2    Specify drop probability for drop precedence level 2
(config)# qos wred queue 0 min-th 20 mdp-1 30 mdp-2 ?
    <0-100>    Specific drop probability in percent
(config)# qos wred queue 0 min-th 20 mdp-1 30 mdp-2 10 ?
    mdp-3    Specify drop probability for drop precedence level 3
(config)# qos wred queue 0 min-th 20 mdp-1 30 mdp-2 10 mdp-3 ?
    <0-100>    Specific drop probability in percent
(config)# qos wred queue 0 min-th 20 mdp-1 30 mdp-2 10 mdp-3 20 ?
    <cr>
(config)# qos wred queue 0 min-th 20 mdp-1 30 mdp-2 10 mdp-3 20
(config)# do show qos wred
qos wred:
=========
Queue  Mode      Min Th  Mdp 1  Mdp 2  Mdp 3
-----  --------  ------  -----  -----  -----
    0  enabled       20     30     10     20
    1  disabled       0      1      5     10
    2  disabled       0      1      5     10
    3  disabled       0      1      5     10
    4  disabled       0      1      5     10
    5  disabled       0      1      5     10

(config)#
```

Drop Precedence Level: every incoming frame is classified to a Drop Precedence Level (DP level) which is used throughout the S4224 to provide congestion control guarantees to the frame according to what was configured for that specific DP level. A DP level of 0 (zero) corresponds to 'Committed' (Green) frames and a DP level of 1 or higher corresponds to 'Discard Eligible' (Yellow) frames.

Weighted Random Early Detection (WRED) is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level (Drop Precedence Level) is used as input to WRED. A higher DP level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

Drop Probability versus Fill Level

The figure below shows the drop probability function with associated parameters.



Max DP 1-3 is the drop probability when the average queue filling level is 100%.

Frames marked with Drop Precedence Level 0 are never dropped.

Min is the average queue filling level where the queues randomly start dropping frames.

The drop probability for frames marked with Drop Precedence Level n increases linearly from zero (at Min average queue filling level) to Max DP n (at 100% average queue filling level).

Command: Configure RADIUS Server(s)

Syntax: **config radius-server**

Description: Configure one to five RADIUS Servers. Authorization is for authorizing users to access the management interfaces of the switch. Note that the RADIUS authentication servers are used both by the NAS module and to authorize access to the switch's management interface. The RADIUS accounting servers are only used by the NAS module.

Mode: (config)#

Example: Display the configuable parameters:

```
(config)# radius-server ?
    attribute     NAS attributes
    deadtime      Time to stop using a RADIUS server that doesn't respond
    host          Specify a RADIUS server
    key           Set RADIUS encryption key
    retransmit    Specify the number of retries to active server
    timeout       Time to wait for a RADIUS server to reply
(config)# radius-server?
radius-server attribute 32 <id>
radius-server attribute 4 <ipv4>
radius-server attribute 95 <ipv6>
radius-server deadtime <minutes>
radius-server host <host_name> [ auth-port <auth_port> ] [ acct-port <acct_port> ] [ timeout
<seconds> ] [ retransmit <retries> ] [ key <key> ]
radius-server key <key>
radius-server retransmit <retries>
radius-server timeout <seconds>
(config)# radius-server host one ?
    acct-port     UDP port for RADIUS accounting server
    auth-port     UDP port for RADIUS authentication server
    key           Server specific key (overrides default)
    retransmit    Specify the number of retries to active server (overrides default)
    timeout       Time to wait for this RADIUS server to reply (overrides default)
    <cr>
(config)# radius-server host one ?
    acct-port     UDP port for RADIUS accounting server
    auth-port     UDP port for RADIUS authentication server
    key           Server specific key (overrides default)
    retransmit    Specify the number of retries to active server (overrides
                  default)
    timeout       Time to wait for this RADIUS server to reply (overrides
                  default)
    <cr>
(config)# radius-server host one acct-port ?
    <AcctPort : 0-65535>    UDP port number
(config)# radius-server host one acct-port 3240 ?
    auth-port     UDP port for RADIUS authentication server
    key           Server specific key (overrides default)
    retransmit    Specify the number of retries to active server (overrides
                  default)
    timeout       Time to wait for this RADIUS server to reply (overrides
                  default)
    <cr>
(config)# radius-server host one acct-port 3240 auth-port ?
    <AuthPort : 0-65535>    UDP port number
(config)# radius-server host one acct-port 3240 auth-port 550 ?
    key           Server specific key (overrides default)
    retransmit    Specify the number of retries to active server (overrides
                  default)
    timeout       Time to wait for this RADIUS server to reply (overrides
                  default)
    <cr>
```

```
(config)# radius-server host one acct-port 3240 auth-port 550 key ?
    <Key : line1-63>    The shared key
(config)# radius-server host one acct-port 3240 auth-port 550 key 12345678 ?
    <Key : line1-63>    The shared key
    retransmit          Specify the number of retries to active server
                        (overrides default)
    timeout             Time to wait for this RADIUS server to reply (overrides
                        default)
    <cr>
(config)# $ver host one acct-port 3240 auth-port 550 key 12345678 retr
<Key : line1-63>  retransmit        timeout           <cr>
(config)# $ver host one acct-port 3240 auth-port 550 key 12345678 retr
<Key : line1-63>  retransmit        timeout           <cr>
(config)# $ver host one acct-port 3240 auth-port 550 key 12345678 retr1 ?
    retransmit          Specify the number of retries to active server
                        (overrides default)
    timeout             Time to wait for this RADIUS server to reply (overrides
                        default)
    <cr>
(config)# $ver host one acct-port 3240 auth-port 550 key 12345678 retr 1 ?
    <Key : line1-63>    The shared key
    retransmit          Specify the number of retries to active server
                        (overrides default)
    timeout             Time to wait for this RADIUS server to reply (overrides
                        default)
    <cr>
(config)# $ver host one acct-port 3240 auth-port 550 key 12345678 retr
<Key : line1-63>  retransmit        timeout           <cr>
(config)# $ne acct-port 3240 auth-port 550 key 12345678 retransmit 1 ?
    <Key : line1-63>    The shared key
    retransmit          Specify the number of retries to active server
                        (overrides default)
    timeout             Time to wait for this RADIUS server to reply (overrides
                        default)
    <cr>
(config)# $ne acct-port 3240 auth-port 550 key 12345678 retransmit 1 time
<Key : line1-63>  retransmit        timeout           <cr>
(config)#
```

RADIUS Parameters:

attribute 4 (NAS-IP-Address): The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used. Must be a valid IP v4 address in dotted decimal notation (“x.y.z.w”), where x, y, z, and w are decimal numbers between 0 and 255.

attribute 95 (NAS-IPv6-Address): The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used. Must be a valid IPv6 address in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon (□ separating each field.

deadtime, which can be set to a number between 0 to 1440 minutes, 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 Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

attribute 32 (NAS-Identifier): The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

host: specify a RADIUS server's parameters:
hostname - The IP address or hostname of the RADIUS server. Must be unique if configuring multiple servers.
auth port - The UDP port to use on the RADIUS server for authentication. Must be unique if configuring multiple servers.
acct port - The UDP port to use on the RADIUS server for accounting. Must be unique if configuring multiple servers.
timeout - This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
retransmit - This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.
key - This optional setting overrides the global key. Leaving it blank will use the global key.

key: the secret key - up to 63 characters long - shared between the RADIUS server and the switch. The authentication messages sent to and from the RADIUS server use an authentication key, not a password. This authentication key, or shared secret, must be the same on the RADIUS client and server. Without this key, there is no communication between the client and server.

retransmit: the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.

timeout: the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.

Command: Configure RMON

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

Description: The S4224 RMON (Remote Network Monitoring) function supports the monitoring and protocol analysis of a LAN per IETF RFC 1271. A part of SNMP, RMON is a network management protocol that gathers remote network information. RMON collects nine kinds of information, including packets sent, bytes sent, packets dropped, statistics by host, by conversations between two sets of addresses, and certain kinds of events that occurred. A network administrator can find out how much bandwidth or traffic each user is imposing on the network and what web sites are being accessed. Alarms can be set to alert you of impending problems. RMON is designed for "flow-based" monitoring.

alarm : Configure an RMON alarm parameters.
event : Configure an RMON event description / log / trap.

Mode: (config)#

Example 1: Display the various configure RMON parameters:

```
(config)# rmon alarm ?
    <1-65535>    Alarm entry ID
(config)# rmon alarm 1 ?
    ifInDiscards         The number of inbound packets that are discarded even if
                         the packets are normal
    ifInErrors           The number of inbound packets that contained errors preventing
                         them from being deliverable to a higher-layer protocol
    ifInNUcastPkts       The number of broad-cast and multi-cast packets
                         delivered to a higher-layer protocol
    ifInOctets           The total number of octets received on the interface,
                         including framing characters
    ifInUcastPkts        The number of uni-cast packets delivered to a higher-layer protocol
    ifInUnknownProtos    The number of the inbound packets that were discarded
                         because of the unknown or un-support protocol
    ifOutDiscards        The number of outbound packets that are discarded even if the
                         packets are normal
    ifOutErrors          The The number of outbound packets that could not be transmitted
                         because of errors
    ifOutNUcastPkts      The number of broad-cast and multi-cast packets that
                         request to transmit
    ifOutOctets          The number of octets transmitted out of the interface, including
                         framing characters
    ifOutUcastPkts       The number of uni-cast packets that request to transmit
(config)# rmon event ?
    <1-65535>    Event entry ID
(config)# rmon event 1 ?
    description    Specify a description of the event
    log            Generate RMON log when the event fires
    trap           Generate SNMP trap when the event fires
    <cr>
(config)# rmon event 1 descr ?
    LINE    Event description
(config)# rmon event 1 log ?
    description    Specify a description of the event
    trap           Generate SNMP trap when the event fires
    <cr>
(config)# rmon event 1 trap ?
    <word127>    SNMP community string
```

Example: 2 Configure the various configure RMON parameters:

```
(config)# rmon alarm 1 ifInErrors ?
    <uint>    ifIndex
(config)# rmon alarm 1 ifInErrors
<uint>
(config)# rmon alarm 1 ifInErrors 1 ?
    <1-2147483647>    Sample interval
(config)# rmon alarm 1 ifInErrors 1 1 ?
    absolute    Test each sample directly
    delta       Test delta between samples
(config)# rmon alarm 1 ifInErrors 1 1 absolute ?
    rising-threshold    Configure the rising threshold
(config)# rmon alarm 1 ifInErrors 1 1 absolute rising-threshold ?
    <-2147483648-2147483647>    rising threshold value
(config)# rmon alarm 1 ifInErrors 1 1 absolute rising-threshold 1000000 ?
    <0-65535>            Event to fire on rising threshold crossing
    falling-threshold    Configure the falling threshold
(config)# $rors 1 1 absolute rising-threshold 1000000 falling-threshold 2000 ?
    <0-65535>    Event to fire on falling threshold crossing
    both         Trigger alarm when the first value is larger than the rising
                 threshold or less than the falling threshold (default)
    falling      Trigger alarm when the first value is less than the falling
                 threshold
    rising       Trigger alarm when the first value is larger than the rising
                 threshold
    <cr>
(config)# $lute rising-threshold 1000000 falling-threshold 2000 falling ?
    <cr>
(config)# $lute rising-threshold 1000000 falling-threshold 2000 falling
(config)#
```

RMON Parameters:

ID: Indicates / set the port index of the entry. The valid range is 1 to 65535.
Interval: Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The valid range is 1 to 2^31-1.
Variable: 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:
InOctets: The total number of octets received on the interface, including framing characters.
InUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol.
InNUcastPkts: The number of broadcast and multi-cast packets delivered to a higher-layer protocol.
InDiscards: The number of inbound packets that are discarded even the packets are normal.
InErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
InUnknownProtos: the number of the inbound packets that were discarded because of the unknown or un-support protocol.
OutOctets: The number of octets transmitted out of the interface, including framing characters.
OutUcastPkts: The number of unicast packets that request to transmit.
OutNUcastPkts: The number of broadcast and multi-cast packets that request to transmit.
OutDiscards: The number of outbound packets that are discarded in the event the packet is normal.
OutErrors: The number of outbound packets that could not be transmitted because of errors.
OutQLen: The length of the output packet queue (in packets).

Sample Type: The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:
Absolute: Get the sample directly.
Delta: Calculate the difference between samples (default).
Value: The value of the statistic during the last sampling period.

Startup Alarm: The method of sampling the selected variable and calculating the value to be compared against the thresholds. The valid sample types are:
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.
RisingOrFalling: Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).
Rising Threshold: Rising threshold value (-2147483648 - 2147483647). The Rising Threshold must be larger than the Falling Threshold.
Rising Index: Rising event index (1 - 65535). The Rising Threshold must be larger than the Falling Threshold.
Falling Threshold: Falling threshold value (-2147483648 - 2147483647). The Falling Threshold must be smaller than the Rising Threshold.
Falling Index: Falling event index (1 - 65535). The Falling Index must be smaller than the Rising Index.

Event Type: Indicates the notification of the event, the valid types are:
none: No logging action is performed.
log: A syslog entry is added.
snmptrap: A SNMP trap event is sent.
logandtrap: A syslog entry is logged and an SNMP trap event is sent.
Community: Specify the community when a trap is sent; the string length is 0 to 127 characters. The default is "public".
Event Last Time: Indicates the value of sysUpTime at the time this event entry last generated an event (e.g., 33554560 or 33 days, 55 hours, 45 minutes, and 50 seconds).

Related RMON RFCs

RFC 2819 - RMON1 - Remote Network Monitoring Management Information Base.

RFC 4502 - RMON2 - Remote Network Monitoring Management Information Base Ver 2 using SMIv2.

RFC 2613 - SMON - Remote Network Monitoring MIB Extensions for Switched Networks.

RFC 3577 - Overview - Introduction to the RMON Family of MIB Modules.

Command: Configure Shared Port

Syntax: **sharedport** { internal | external }

Description: Configure the FPGA Shared Port status to internal or external.

This switch contains one port that is 'Shared'. On S4212 products, it's port 12, and on S4224 products, it's port 24. The Shared Port has two mode to work. One mode is '**External**', the port can work as normal port. The other mode is '**Internal**', the port is just used for 2544 testing, and it is not user configurable.

Set the Shared Port operation. Possible modes are:

Internal: This mode disconnects the the Shared Port from the SFP interface and attaches it internally to to an FPGA. No connectivity can be achieved through the Shared Port's SFP interface while in this mode.

External: This is the default mode. In this mode, the shared port is attached to the SFP interface, and works like the rest of the ports on this switch.

The Shared Port mode must be set to '**External**' for normal port function and '**Internal**' for the following features to work:

Diagnostics > **Service Activation** > **Test**

Diagnostics > **Service Activation** > **Loopback**

Mode: (config)#

Example 1: Set the FPGA Shared Port status to internal and external.

```
(config)# sharedport ?
    external
    internal
(config)# sharedport?
    sharedport    Shared Port status: Internal or External
(config)# sharedport??
sharedport { internal | external }
(config)# sharedport?
    sharedport    Shared Port status: Internal or External
(config)# sharedport internal ?
    <cr>
(config)# sharedport external ?
    <cr>
(config)# sharedport external
(config)# sharedport internal
(config)#
```

Command: Configure SNMP Server

Syntax: **config snmp**

Description: Configure SNMP Server parameters.

Mode: (config)#

Example 1: Display the SNMP server functions.

```
(config)# snmp ?
    access               access configuration
    community            Set the SNMP community
    contact              Set the SNMP server's contact string
    engine-id            Set SNMP engine ID
    host                 Set SNMP host's configurations
    location             Set the SNMP server's location string
    security-to-group    security-to-group configuration
    trap                 Set trap's configurations
    user                 Set the SNMPv3 user's configurations
    version              Set the SNMP server's version
    view                 MIB view configuration
    <cr>
(config)# snmp
```

Example 2: Display the SNMP configurable parameters.

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

Each SNMP sub-command is described below.

Command: Configure SNMP Server Access (Model and Level)

Syntax: **snmp-server access** <group_name> **model** { v1 | v2c | v3 | any } **level** { auth | noauth | priv } [read <view_name>] [write <write_name>]

Description: Configure SNMP Server parameters and display the resulting config.

Mode: (config)#

Example 1: Configure SNMP Server's Access:

```
(config)# snmp-server access GrNm1 ?
    model    security model
(config)# snmp-server access GrNm1
model
(config)# snmp-server access GrNm1 model ?
    any    any security model
    v1     v1 security model
    v2c    v2c security model
    v3     v3 security model
(config)# snmp-server access GrNm1 model any ?
    level    security level
(config)# snmp-server access GrNm1 model any level ?
    auth      authNoPriv Security Level
    noauth    noAuthNoPriv Security Level
    priv      authPriv Security Level
(config)# snmp-server access GrNm1 model any level auth ?
    read     specify a read view for the group
    write    specify a write view for the group
    <cr>
(config)# snmp-server access GrNm1 model any level auth read ?
    <ViewName : word255>    read view name
(config)# snmp-server access GrNm1 model any level auth read rrr ?
    write    specify a write view for the group
    <cr>
(config)# snmp-server access GrNm1 model any level auth read rrr write ?
    <WriteName : word255>    write view name
(config)# snmp-server access GrNm1 model any level auth read rrr write www ?
    <cr>
(config)# snmp-server access GrNm1 model any level auth read rrr write www
The group name 'GrNm1' is not exist
# show snmp access
Group Name       : default_ro_group
Security Model   : any
Security Level   : NoAuth, NoPriv
Read View Name   : default_view
Write View Name  : <no writeview specified>

Group Name       : default_rw_group
Security Model   : any
Security Level   : NoAuth, NoPriv
Read View Name   : default_view
Write View Name  : default_view

#
```

Command: Configure SNMP Server Version v2c Community

Syntax: **config snmp-server community** v2c <comm> [ro | rw]

Description: Configure SNMP Server SNMP Version to v2c and set RO/RW parameter.

Mode: (config)

Example 1: Configure the SNMP server to SNMP v2c with rw (read and write) access,.

```
(config)# snmp-server community ?
    v2c    SNMPv2c
    v3     SNMPv3
(config)# snmp-server community v2c ?
    <Comm : word255>    Community word
(config)# snmp-server community v2c?
    v2c    SNMPv2c
(config)# snmp-server community v2c?
snmp-server community v2c <comm> [ ro | rw ]
(config)# snmp-server community v2c comm ?
    ro      Read only
    rw      Read write
    <cr>
(config)# snmp-server community v2c comm rw ?
    <cr>
(config)# snmp-server community v2c comm rw
(config)# snmp-server community
```

***Read* Community** indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

***Write* Community** indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Command: Configure SNMP Server Community Version v3

Syntax: **snmp-server community v3** <v3_comm> [<v_ipv4_addr> <v_ipv4_netmask>]

Description: Configure SNMP Server SNMP v3 parameters.

Mode: (config)#

Example 1: Configure the SNMP server to SNMP v3 with an IPv4 address and netmask, and then display the resulting config.

```
(config)# snmp-server community ?
    v2c    SNMPv2c
    v3     SNMPv3
(config)# snmp-server community v3 ?
    <V3Comm : word32>    Community word
(config)# snmp-server community v3 comm3 ?
    <ipv4_addr>    IPv4 address
    <cr>
(config)# snmp-server community v3 comm3 192.168.1.30 ?
    <ipv4_netmask>    IPv4 netmask
(config)# snmp-server community v3 comm3 192.168.1.30 255.255.255.0 ?
    <cr>
(config)# snmp-server community v3 comm3 192.168.1.30 255.255.255.0
(config)# end
# show snmp community v3
Community   : public
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0

Community   : private
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0

Community   : comm3
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0

#
```

Command: Configure SNMP Server Contact Info

Syntax: **snmp-server contact** <line255>

Description: Set the SNMP server's contact string.

Mode: (config)#

Example 1: Configure the SNMP server contact information.

```
(config)# snmp-server contact jeffs@transition.com
(config)#
```

Command: Configure SNMP Server Local Engine ID

Syntax: **snmp-server engine-id local** <engineID>

Description: Configure SNMP Server local engine id parameter (e.g., *800007e5017f000001*).
The SNMPv3 engine ID string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.
Changing the Engine ID will clear all original local users.

Mode: (config)#

Example 1: Configure the SNMP local engine ID.

```
(config)# snmp engine-id ?
    local    Set SNMP local engine ID
(config)# snmp engine-id local ?
    <Engineid : word10-32>    local engine ID
(config)# snmp engine-id local 800007e5017f000001
(config)#
```

Command: Configure SNMP Server Host

Syntax: **snmp-server host** <conf_name>

Description: Set SNMP host's configurations.

Mode: (config)#

Example 1: Configure the SNMP server *host1*.

```
(config)# snmp-server host host1?
    <word32>    Name of the host configuration
    <cr>
(config)# snmp-server host host1 ?
    <cr>
(config)# snmp-server host host1
(config-snmps-host)# ?
    do          To run exec commands in config mode
    end         Go back to EXEC mode
    exit        Exit from current mode
    help        Description of the interactive help system
    host        host configuration
    informs     Send Inform messages to this host
    no          Negate a command or set its defaults
    shutdown    Disable the trap configuration
    traps       trap event configuration
    version     Set SNMP trap version
(config-snmps-host)# host ?
    <hostname>      hostname of SNMP trap host
    <ipv4_ucast>    IP address of SNMP trap host
    <ipv6_ucast>    IP address of SNMP trap host
(config-snmps-host)# informs ?
    retries    retires inform messages
(config-snmps-host)# shutdown ?
    <cr>
(config-snmps-host)# traps ?
    aaa       AAA event group
    switch    Switch event group
    system    System event group
    <cr>
(config-snmps-host)# traps system ?
    aaa          AAA event group
    coldstart    Cold start event
    switch       Switch event group
    warmstart    Warm start event
```

```
    <cr>
(config-snmps-host)# version ?
    v1    SNMP trap version 1
    v2    SNMP trap version 2
    v3    SNMP trap version 3
(config-snmps-host)#
```

Command: Configure SNMP Server Location

Syntax: **snmp-server location** <v_line255>

Description: Set the location (address, building, floor, etc) of the SNMP server.

Mode: (config)#

Example 1: Set the SNMP server's location:

```
(config)# snmp-server location ?
    <line255>    location string
(config)# snmp-server location 1234 Home Ave., Mtka, MN 55344
(config)#
```

Command: Configure SNMP Server Security

Syntax: **snmp-server security-to-group model** { v1 | v2c | v3 } name <security_name> group <group_name>

Description: Set SNMP server's security-to-group model .

Mode: (config)

Example 1: Configure the SNMP server security model for a group or groups.

```
(config)# snmp-server security-to-group model ?
    v1     v1 security model
    v2c    v2c security model
    v3     v3 security model
(config)# snmp-server security-to-group model v3 ?
    name    security user
(config)# snmp-server security-to-group model v3 name ?
    <SecurityName : word32>    security user name
(config)# snmp-server security-to-group model v3 name jeffs ?
    group    security group
(config)# snmp-server security-to-group model v3 name jeffs group ?
    <GroupName : word32>    security group name
(config)# snmp-server security-to-group model v3 name jeffs group eng ?
    <cr>
(config)# snmp-server security-to-group model v3 name jeffs group eng
(config)# end
# show snmp security-to-group
Security Model : v1
Security Name  : public
Group Name     : default_ro_group

Security Model : v1
Security Name  : private
Group Name     : default_rw_group

Security Model : v2c
Security Name  : public
Group Name     : default_ro_group

Security Model : v2c
```

```
Security Name  : private
Group Name     : default_rw_group

Security Model : v3
Security Name  : jeffs
Group Name     : eng

Security Model : v3
Security Name  : default_user
Group Name     : default_rw_group

#
```

Command: Configure SNMP Server Trap

Syntax: **snmp-server trap**

Description: Set SNMP server's trap configuration.

Mode: (config)

Example 1: Configure the SNMP server trap.

```
(config)# snmp trap?
snmp-server trap
(config)# snmp trap
(config)#
```

Command: Configure SNMP Server Users

Syntax: **snmp-server user** <username> engine-id <engineID> [{ md5 <md5_passwd> | sha <sha_passwd> } [priv { des | aes } <priv_passwd>]]

Description: Set the SNMPv3 user's configurations. See below for descriptions.

<**username**> the configured user name.

<**engineID**> e.g., snmp engine-id local = 800007e5017f000001

< **md5**>|<**sha**> Set MD5 protocol or set SHA protocol.

<**md5_passwd**> MD5 password if MD5 selected (8-32 character word).

<**sha_passwd**> SHA password if SHA selected (8-49 character word).

priv { **des** | **aes** } Set privacy to DES or AES.

<**priv_passwd**> Set privacy password.

Mode: (config)

Example 1: Configure SNMP server User “jeffs” and display the resulting config.

```
(config)# snmp user ?
    <word32>    Username
(config)# snmp user jeffs ?
    engine-id    engine ID
(config)# snmp user jeffs engine-id 800007e5017f000001 ?
    md5     Set MD5 protocol
    sha     Set SHA protocol
    <cr>
(config)# snmp user jeffs engine-id 800007e5017f000001
(config)# snmp user jeffs engine-id 800007e5017f000001 sha ShaPasswd ?
    priv    Set Privacy
    <cr>
(config)# $p user jeffs engine-id 800007e5017f000001 sha ShaPasswd priv ?
    aes    Set AES protocol
    des    Set DES protocol
(config)# $p user jeffs engine-id 800007e5017f000001 sha ShaPasswd priv aes ?
    <word8-32>    Set privacy password
(config)# $fs engine-id 800007e5017f000001 sha ShaPasswd priv aes AesPasswd ?
    <cr>
(config)# $fs engine-id 800007e5017f000001 sha ShaPasswd priv aes AesPasswd
(config)# end
# show snmp user jeffs 800007e5017f000001 ?
    |       Output modifiers
    <cr>
# show snmp user jeffs 800007e5017f000001
User Name               : jeffs
Engine ID               : 800007e5017f000001
Security Level          : Auth, Priv
Authentication Protocol : SHA
Privacy Protocol        : DES

#
```

SNMP Parameter Descriptions

Engine ID: An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.

User Name: A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Level: Indicates the security model that this entry should belong to. Valid security models are:
NoAuth, NoPriv: No authentication and no privacy.
Auth, NoPriv: Authentication and no privacy.
Auth, Priv: Authentication and privacy.

The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.

Authentication Protocol: Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

None: No authentication protocol.
MD5: An optional flag to indicate that this user uses MD5 authentication protocol.
SHA: An optional flag to indicate that this user uses SHA authentication protocol.

The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.

Authentication Password: A string identifying the authentication password phrase. For the MD5 authentication protocol, the allowed string length is 8 to 32. For the SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.

Privacy Protocol: Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

None: No privacy protocol.
DES: An optional flag to indicate that this user uses DES authentication protocol.
AES: An optional flag to indicate that this user uses AES authentication protocol.

Privacy Password: A string identifying the privacy password phrase. The allowed string length is 8 to 32 characters, and the allowed content is ASCII characters from 33 to 126.

Command: Configure SNMP Server Version

Syntax: **snmp-server version** { v1 | v2c | v3 }

Description: Set the SNMP server version.

Mode: (config)

Example 1: Configure the SNMP server' SNMP version.

```
(config)# snmp-server version v1
(config)# snmp-server version v2
(config)# snmp-server version v3
(config)#
```

Command: Configure SNMP Server MIB View

Syntax: **snmp-server view** <view_name> <oid_subtree> { include | exclude }

Description: Set SNMP server's MIB view configuration. The first character must be a dot (.) character.

Mode: (config)

Example 1: Configure the SNMP server MIB view configuration and display the resulting info.

```
(config)# snmp view ?
    < word32>    MIB view name
(config)# snmp view 1 DSFDD ?
    exclude    Excluded type from the view
    include    Ixcluded type from the view
(config)# snmp view default_view 1 include ?
    <cr>
(config)# snmp view default_view 1 include
first character must be '.'
(config)# snmp view default_view ?
    <OidSubtree : word255>    MIB view OID
(config)# snmp view default_view 1 include
first character must be '.'
(config)# snmp view default_view .1 include
(config)# end
# show snmp view
View Name   : default_view
OID Subtree : .1
View Type   : included
(config)# snmp view default_view .1 exclude
(config)# do show snmp view
View Name   : default_view
OID Subtree : .1
View Type   : excluded

(config)#
```

Command: Configure Spanning Tree

Syntax: **config spanning-tree**

Description: Configure Spanning Tree protocol parameters. The S4224 supports Spanning Tree versions IEEE 802.1D STP, 802.1w RSTP, and 802.1s MSTP. MSTP is selected by default. The IEEE 802.1s standard supports 16 instances. Note that STP on MGMT / Port 1 is disabled by default.
The S4224 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 S4224 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 S4224 also supports configuration options for enabling/disabling BPDU guard, path cost for that port, restricting topology change notification, etc.

Mode: (config)#

Example 1: Display the Spanning Tree functions available.

```
(config)# spanning-tree ?
    aggregation    Aggregation mode
    edge           Edge ports
    mode           STP protocol mode
    mst            STP bridge instance
    recovery       The error recovery timeout
    transmit       BPDUs to transmit
(config)# spanning-tree??
spanning-tree aggregation
spanning-tree edge bpdu-filter
spanning-tree edge bpdu-guard
spanning-tree mode { stp | rstp | mstp }
spanning-tree mst <instance> priority <prio>
spanning-tree mst <instance> vlan <v_vlan_list>
spanning-tree mst forward-time <fwdtime>
spanning-tree mst max-age <maxage> [ forward-time <fwdtime> ]
spanning-tree mst max-hops <maxhops>
spanning-tree mst name <name> revision <v_0_to_65535>
spanning-tree recovery interval <interval>
spanning-tree transmit hold-count <holdcount>
(config)# spanning-tree
```

Example 2: Display the Spanning Tree sub-functions.

```
(config)# spanning-tree ?
    aggregation    Aggregation mode
    edge           Edge ports
    mode           STP protocol mode
    mst            STP bridge instance
    recovery       The error recovery timeout
    transmit       BPDUs to transmit
(config)# spanning-tree aggregation ?
    <cr>
(config)# spanning-tree aggregation
(config-stp-aggr)# ?
    do               To run exec commands in config mode
    end              Go back to EXEC mode
    exit             Exit from current mode
    help             Description of the interactive help system
    no               Negate a command or set its defaults
    spanning-tree    Spanning Tree protocol
(config-stp-aggr)# spanning-tree ?
    auto-edge          Auto detect edge status
    bpdu-guard         Enable/disable BPDU guard
    edge               Edge port
    link-type          Port link-type
    mst                STP bridge instance
    restricted-role    Port role is restricted (never root port)
    restricted-tcn     Restrict topology change notifications
    <cr>
(config-stp-aggr)# end
# con ter
(config)# spanning-tree edge ?
    bpdu-filter    Enable BPDU filter (stop BPDU tx/rx)
    bpdu-guard     Enable BPDU guard
(config)# spanning-tree edge bpdu-filter ?
    <cr>
(config)# spanning-tree edge bpdu-guard ?
    <cr>
(config)# spanning-tree mode ?
    mstp    Multiple Spanning Tree (802.1s)
    rstp    Rabid Spanning Tree (802.1w)
    stp     802.1D Spanning Tree
(config)# spanning-tree mode mstp ?
    <cr>
(config)# spanning-tree mode rstp ?
    <cr>
(config)# spanning-tree mode stp ?
    <cr>

(config)# spanning-tree mst ?
    <Instance : 0-7>    instance  0-7 (CIST=0, MST2=1...)
    forward-time        Delay between port states
    max-age             Max bridge age before timeout
    max-hops            MSTP bridge max hop count
    name                Name keyword
 (config)# spanning-tree mst 1?
    <Instance : 0-7>    instance  0-7 (CIST=0, MST2=1...)
```

```
(config)# spanning-tree mst 1?
spanning-tree mst <instance> priority <prio>
spanning-tree mst <instance> vlan <v_vlan_list>
(config)# spanning-tree mst 1 priority ?
    <Prio : 0-61440>    Range in seconds
(config)# spanning-tree mst 1 vlan ?
    <vlan_list>    Range of VLANs
 (config)# spanning-tree mst 1 vlan?
    vlan    VLAN keyword
(config)# spanning-tree mst 1 vlan?
spanning-tree mst <instance> vlan <v_vlan_list>
(config)# spanning-tree mst 1 vlan ?
    <vlan_list>    Range of VLANs
(config)# spanning-tree mst 1 vlan 1 ?
    <cr>
(config)# spanning-tree mst 1 vlan 1
(config)#
```

Example 3: Configure spanning-tree and display the Spanning Tree summary.

```
# show spanning-tree summary
Protocol Version: MSTP
Max Age         : 20
Forward Delay   : 15
Tx Hold Count   : 6
Max Hop Count   : 20
BPDU Filtering  : Disabled
BPDU Guard      : Disabled
Error Recovery  : Disabled
CIST Bridge is active
# config term
(config)# spanning-tree ?
    aggregation    Aggregation mode
    edge           Edge ports
    mode           STP protocol mode
    mst            STP bridge instance
    recovery       The error recovery timeout
    transmit       BPDUs to transmit
(config)# spanning-tree aggregation
(config)# spanning-tree edge ?
    bpdu-filter    Enable BPDU filter (stop BPDU tx/rx)
    bpdu-guard     Enable BPDU guard
(config)# spanning-tree edge bpdu-filter ?
    <cr>
(config)# spanning-tree edge bpdu-filter
 (config)# spanning-tree edge bpdu-guard
(config)# spanning-tree mode ?
    mstp    Multiple Spanning Tree (802.1s)
    rstp    Rabid Spanning Tree (802.1w)
    stp     802.1D Spanning Tree
(config)# spanning-tree mode rstp
(config)# spanning-tree mode mst
(config)# spanning-tree recovery interval ?
    <Interval : 30-86400>    Range in seconds
(config)# spanning-tree recovery interval 60
(config)# spanning-tree transmit hold-count ?
    <Holdcount : 1-10>    1-10 per sec, 6 is default
(config)# spanning-tree transmit hold-count 3
(config)# end
# show spanning-tree ?
```

```
    |            Output modifiers
    active       STP active interfaces
    detailed     STP statistics
    interface    Choose port
    mst          Configuration
    summary      STP summary
    <cr>
# show spanning-tree summary
Protocol Version: RSTP
Max Age         : 20
Forward Delay   : 15
Tx Hold Count   : 3
Max Hop Count   : 20
BPDU Filtering  : Enabled
BPDU Guard      : Enabled
Error Recovery  : 60 seconds
CIST Bridge is active
#
```

Spanning Tree Parameters Summary

spanning-tree aggregationmode
spanning-tree edge bpdu-filter ; Enable BPDU filter (stop BPDU tx/rx)
spanning-tree edge bpdu-guard ; Enable BPDU guard
spanning-tree mode { stp | rstp | mstp }
spanning-tree mst <instance> priority <prio> Range in seconds <0-61440>
spanning-tree mst <instance> vlan <vlan_list> Range of VLANs
spanning-tree mst forward-time <fwdtime> Range in seconds <4-30>
spanning-tree mst max-age <maxage> [forward-time <fwdtime>]
spanning-tree mst max-hops <maxhops> Hop count range <6-40>
spanning-tree mst name <name> revision <v_0_to_65535>
spanning-tree recovery interval <interval> Range in seconds <30-86400>
spanning-tree transmit hold-count <holdcount> 1-10 per sec, 6 is default

Command: Configure Switch Port

Syntax: **switchport vlan mapping** <gid> <vlan_list> <tvid>

Description: Configure switch port switching mode characteristics. Add VLAN translation entry into a group.

Group ID: The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 28.
Note: By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.
VID: Indicates the VLAN of the mapping (i.e. 'source' VLAN). A valid VLAN ID ranges from 1 to 4095.
TVID: Indicates the VLAN ID to which VLAN ID of an ingress frame will be translated to (granted that the mapping is enabled on the ingress port that the frame arrived at). A valid VLAN ID ranges from 1 to 4095.

Mode: (config)#

Example 1: Configure switchport vlan mapping:

```
(config)# switchport ?
    vlan    vlan - Vlan translation
(config)# switchport?
switchport vlan mapping <gid> <vlan_list> <tvid>
(config)# switchport vlan ?
    mapping    Add VLAN translation entry into a group.
(config)# switchport vlan mapping ?
    <group id : 1-10>    Group id
(config)# switchport vlan mapping 1 ?
    <vlan_list>
(config)# switchport vlan mapping 1 10 ?
    <vlan_id>
(config)# switchport vlan mapping 1 10 1 ?
    <cr>
(config)# switchport vlan mapping 1 10 1
(config)#
```

Messages: *% VLAN ID and Translated VLAN ID cannot be same*

Example 2: Configure switchport VLAN mapping:

```
(config)# switchport vlan mapping 1 1 1
% VLAN ID and Translated VLAN ID cannot be same
(config)# switchport vlan mapping 1 1 2
(config)#
```

Example 3: Configure interface(s) switchport parameters:

```
(config)# interface ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
    <cr>                 VLAN interface configurations
(config)# interface * ?
    <port_type_list>    Port list for all port types
    <cr>
(config)# interface * 1/1-4 ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
```

```
    <cr>
(config)# interface * 1/1-4
(config-if)# switchport ?
    access       Set access mode characteristics of the interface
    forbidden    Adds or removes forbidden VLANs from the current list of
                 forbidden VLANs
    hybrid       Change PVID for hybrid port
    mode         Set mode of the interface
    trunk        Change PVID for trunk port
    vlan         VLAN commands
 (config-if)# switchport?
    switchport    Switching mode characteristics
(config-if)# switchport ?
    access       Set access mode characteristics of the interface
    forbidden    Adds or removes forbidden VLANs from the current list of
                 forbidden VLANs
    hybrid       Change PVID for hybrid port
    mode         Set mode of the interface
    trunk        Change PVID for trunk port
    vlan         VLAN commands
(config-if)# switchport
```

Messages

% VLAN ID and Translated VLAN ID cannot be same

% (VLAN Translation Error - The provided Translation VLAN ID is the same as the VLAN ID - makes no sense to translate a VID to itself)

Parameter Summary

switchport access vlan <pvid>
switchport forbidden vlan { add | remove } <vlan_list>
switchport hybrid acceptable-frame-type { all | tagged | untagged }
switchport hybrid allowed vlan { all | none | [add | remove | except] <vlan_list> }
switchport hybrid egress-tag { none | all [except-native] }
switchport hybrid ingress-filtering
switchport hybrid native vlan <pvid>
switchport hybrid port-type { unaware | c-port | s-port | s-custom-port }
switchport mode { access | trunk | hybrid }
switchport trunk allowed vlan { all | none | [add | remove | except] <vlan_list> }
switchport trunk native vlan <pvid>
switchport trunk vlan tag native
switchport vlan ip-subnet [id <1-128>] <ipv4> vlan <vid>
switchport vlan mac <mac_addr> vlan <vid>
switchport vlan mapping <gid>
switchport vlan protocol group <grp_id> vlan <vid>

Command: Configure TACACS Server

Syntax: **tacacs-server deadtime** <minutes>
tacacs-server host <host_name> [port <port>] [timeout <seconds>] [key <key>]
tacacs-server key <key>
tacacs-server timeout <seconds>

Description: Configure TACACS Server in terms of global TACACS+ server configuration details. You can configure up to 5 TACACS+ Authentication servers. **Note**: TACACS+ servers are only used to authorize access to the S4224 management interface.

Mode: (config)#

Example:

```
(config)# tacacs-server?
    tacacs-server    Configure TACACS+
(config)# tacacs-server ?
    deadtime    Time to stop using a TACACS+ server that doesn't respond
    host        Specify a TACACS+ server
    key         Set TACACS+ encryption key
    timeout     Time to wait for a TACACS+ server to reply
(config)# tacacs-server??
tacacs-server deadtime <1-1440>
tacacs-server key <line1-63>
tacacs-server timeout <1-1000>
 (config)# tacacs-server deadtime ?
    <Minutes : 1-1440>    Time in minutes
 (config)# tacacs-server deadtime 60
(config)# tacacs-server host ?
    <word1-255>    Hostname or IP address
(config)# tacacs-server host 192.168.1.30 ?
    key        Server specific key (overrides default)
    port       TCP port for TACACS+ server
    timeout    Time to wait for this TACACS+ server to reply (overrides default)
    <cr>
(config)# tacacs-server key ?
    <Key : line1-63>    The shared key
(config)# tacacs-server ?
    deadtime    Time to stop using a TACACS+ server that doesn't respond
    host        Specify a TACACS+ server
    key         Set TACACS+ encryption key
    timeout     Time to wait for a TACACS+ server to reply
(config)# tacacs-server timeout ?
    <Seconds : 1-1000>    Wait time in seconds
(config)# tacacs-server timeout 360
(config)#
```

Deadtime is the period (0 to 1440 minutes) 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 Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

Key is the secret key (password) which can be up to 63 characters long and is shared between the TACACS+ server and the switch.

Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.

Command: Configure Terminal Mode

Syntax: **configure terminal**

Description: Changes the S4224 to "config" mode where you can configure the major features and functions.

Mode: *(config)#*

Example: Display the configurable functions:

```
# config terminal
    aaa              Authentication, Authorization and Accounting
    access           Access management
    access-list      Access list
    aggregation      Aggregation mode
    banner           Define a login banner
    clock            Configure time-of-day clock
    ddmi             DDMI Information
    default          Set a command to its defaults
    do               To run exec commands in config mode
    dot1x            IEEE Standard for port-based Network Access Control
    enable           Modify enable password parameters
    end              Go back to EXEC mode
    eps              Ethernet Protection Switching.
    erps             Ethernet Ring Protection Switching
    ethersat         ethersat (Service Activation Test)
    evc              Ethernet Virtual Connections
    exit             Exit from current mode
    gvrp             Enable GVRP feature
    help             Description of the interactive help system
    hostname         Set system's network name
    interface        Select an interface to configure
    ip               Internet Protocol
    ipmc             IPv4/IPv6 multicast configuration
    ipv6             IPv6 configuration commands
    lacp             LACP settings
    line             Configure a terminal line
    lldp             LLDP configurations.
    logging          System logging message
    loop-protect     Loop protection configuration
    mac              MAC table entries/configuration
    mep              Maintenance Entity Point
    monitor          Monitoring different system events
    mvr              Multicast VLAN Registration configuration
    network-clock    network-clock
    no               Negate a command or set its defaults
    ntp              Configure NTP
    perf-mon         Performance Monitor
    port-security    Enable/disable port security globally.
    privilege        Command privilege parameters
    ptp              Precision time Protocol (1588)
    qos              Quality of Service
    radius-server    Configure RADIUS
    rmon             Remote Monitoring
    sharedport       Shared Port status: Internal or External
    snmp-server      Set SNMP server's configurations
    spanning-tree    Spanning Tree protocol
    switchport       Set switching mode characteristics
    tacacs-server    Configure TACACS+
    udld             Enable UDLD in the aggressive or normal mode and to set
                     the configurable message timer on all fiber-optic ports.
    username         Establish User Name Authentication
    vlan             VLAN commands
    web              Web
```

Related commands: **do** To run exec commands in config mode. end Go back to EXEC mode.
exit Exit from current mode.

Command: Configure UDLD

Syntax: **udld** { aggressive | enable | message time-interval <v_interval> }

Description: Enable UDLD in the aggressive or normal mode and set the configurable message timer on all fiber-optic ports. The UDLD (Uni Directional Link Detection) protocol monitors the physical configuration of the links between devices and ports that support UDLD. UDLD detects the existence of unidirectional links.Its functionality is to provide mechanisms useful for detecting one way connections before they create a loop or other protocol malfunction. IETF RFC 5171 specifies a way at data link layer to detect a Uni-directional link.

Mode: (config)#

Example: Display the **udld** command functions, configure udld, and display the resulting config:

```
(config)# udld ?
    aggressive    Enables UDLD in aggressive mode on all fiber-optic ports.
    enable        Enables UDLD in normal mode on all fiber-optic ports.
    message       Configures the period of time between UDLD probe messages on
                  ports that are in the advertisement phase and are determined
                  to be bidirectional. The range is from 7 to 90 seconds. (Currently
                   default message time interval 7 sec is supported).
(config)# udld aggressive
(config)# udld enable
(config)# udld message ?
    time-interval    Configures the period of time between UDLD probe messages
                     on ports that are in the advertisement phase and are
                     determined to be bidirectional. The range is from 7 to 90
                     seconds.
(config)# udld message time-interval ?
    <7-90>    Configures the period of time between UDLD probe messages on
              ports that are in the advertisement phase and are determined to
              be bidirectional. The range is from 7 to 90 seconds. (Currently
              default message time interval 7 sec is supported).
(config)# udld message time-interval 10 ?
    <cr>
(config)# udld message time-interval 10
(config)# end
# show udld

GigabitEthernet 1/1
---------------------------------------------------------------------
UDLD Mode                 : Normal
Admin State               : Enable
Message Time Interval(Sec): 10
Device ID(local)          : 00-C0-F2-56-1A-90
Device Name(local)        :
Bidirectional state       : Indeterminant

No neighbor cache information stored
--------------------

GigabitEthernet 1/2
---------------------------------------------------------------------
UDLD Mode                 : Normal
Admin State               : Enable
Message Time Interval(Sec): 10
Device ID(local)          : 00-C0-F2-56-1A-90
Device Name(local)        :
Bidirectional state       : Indeterminant
-- more --, next page: Space, continue: g, quit: ^C
```

Command: Configure Username Authentication

Syntax: **username**

Description: Establish User Name Authentication.

encrypted Specifies an ENCRYPTED password will follow. The ENCRYPTED (hidden) user password. Notice the ENCRYPTED password will be decoded by system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally. <**Password** : word4-44>

none NULL password.

unencrypted Specifies an UNENCRYPTED password will follow. The UNENCRYPTED (Plain Text) user password. Any printable characters including space is accepted. Notice that you have no chance to get the Plain Text password after this command. The system will always display the ENCRYPTED password. <**Password** : line31>

Mode: (config)#

Example:

```
(config)# username ?
<word31>    User name allows letters, numbers and underscores
(config)# username??
username <username> privilege <priv> password encrypted <encry_password>
username <username> privilege <priv> password none
username <username> privilege <priv> password unencrypted <password>
(config)# username admin2 ?
    privilege    Set user privilege level
(config)# username admin2 privilege ?
    <privilegeLevel : 0-15>    User privilege level
(config)# username admin2 privilege 14 ?
    password    Specify the password for the user
(config)# username admin2 privilege 14 password ?
    encrypted      Specifies an ENCRYPTED password will follow
    none           NULL password
    unencrypted    Specifies an UNENCRYPTED password will follow
(config)# username admin2 privilege 14 password unencrypted ?
    <line31>    The UNENCRYPTED (Plain Text) user password. Any printable
                characters including space is accepted. Notice that you
                have no chance to get the Plain Text password after this
                command. The system will always display the ENCRYPTED
                password.
(config)# username admin2 privilege 14 password unencrypted ?
username <username> privilege <priv> password unencrypted <password>
(config)# username admin2 privilege 14 password unencrypted Buffrey32 ?
username <username> privilege <priv> password unencrypted <password>
(config)# username admin2 privilege 14 password unencrypted Buffrey32
```

Command: Configure VLAN

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

Description: Configure VLAN (Virtual LAN) parameters. The IEEE 802.1Q standard VLANs are supported and the default configuration is as follows:

- All ports are VLAN aware;
- All ports are members of VLAN 1;
- The switch management interface is on VLAN 1;
- All ports have a Port VLAN ID (PVID) of 1; and
- All ports can send and receive both VLAN-tagged and untagged packets

In the default configuration, any port is able to send traffic to any other port, and a PC connected to any port will be able to reach the management interface. Broadcast traffic, for example, will be flooded to all ports on the switch.
Note: VLAN 1 is reserved for the default VLAN. The VLAN ID valid range is 2 - 4095.
Note: the <vlan_list> or <vlist> parameter sets the Global VLAN Configuration for Allowed Access VLANs (e.g., VLANs 1-4,10,100).

Mode: (config)#

Example 1: Configure VLAN EtherType and protocol parameters:

```
(config)# vlan ?
    <vlan_list>    ISL VLAN IDs 1~4095
    ethertype      Ether type for Custom S-ports
    protocol       Protocol-based VLAN commands
(config)# vlan?
vlan <vlan_list>
vlan ethertype s-custom-port <0x0600-0xffff>
vlan protocol { { eth2 { <0x600-0xffff> | arp | ip | ipx | at } } | { snap { <0x0-0xffffff> |
rfc_1042 | snap_8021h } <0x0-0xffff> } | { llc <0x0-0xff> <0x0-0xff> } } group <word16>
(config)# vlan ethertype ?
    s-custom-port    Custom S-ports configuration
(config)# vlan protocol ?
    eth2    Ethernet-based VLAN commands
    llc     LLC-based VLAN group
    snap    SNAP-based VLAN group
(config)# vlan protocol eth2 ?
    <0x600-0xffff>    Ether Type(Range: 0x600 - 0xFFFF)
    arp               Ether Type is ARP
    at                Ether Type is AppleTalk
    ip                Ether Type is IP
    ipx               Ether Type is IPX
(config)# vlan protocol llc ?
    <0x0-0xff>    DSAP (Range: 0x00 - 0xFF)
(config)# vlan protocol snap ?
    <0x0-0xffffff>    SNAP OUI (Range 0x000000 - 0XFFFFFF)
    rfc-1042          SNAP OUI is rfc-1042
    snap-8021h        SNAP OUI is 8021h
(config)# vlan protocol snap
(config)# vlan 1
(config-vlan)# ?
    do      To run exec commands in config mode
    end     Go back to EXEC mode
    exit    Exit from Configuration VLAN mode
    help    Description of the interactive help system
    name    ASCII name of the VLAN
    no
(config-vlan)#
```

Example 2: Configure various VLAN parameters:

```
(config)# vlan 1?
    <vlan_list>    ISL VLAN IDs 1~4095
    <cr>
(config)# vlan 1
(config-vlan)# ?
    do      To run exec commands in config mode
    end     Go back to EXEC mode
    exit    Exit from current mode
    help    Description of the interactive help system
    name    ASCII name of the VLAN
    no
(config-vlan)# do ?
    LINE    Exec Command
(config-vlan)# do?
    do    To run exec commands in config mode
(config-vlan)# do?
do <command>
(config-vlan)# do end ?
    LINE    Exec Command
    <cr>
(config-vlan)# do end?
    LINE    Exec Command
    <cr>
(config-vlan)# do exit ?
    LINE    Exec Command
    <cr>
(config-vlan)# do help ?
    LINE    Exec Command
    <cr>
(config-vlan)# do name?
    LINE    Exec Command
    <cr>
(config-vlan)# do name?
    LINE    Exec Command
    <cr>
(config-vlan)# do name?
do <command>
(config-vlan)# do name
```

Example 3: VLAN name cannot contain the space character:

```
(config-vlan)# name ABC!@#123 XYZ
                              ^
% Invalid word detected at '^' marker.

(config-vlan)#
```

VLAN Notes

A **Port based** VLAN is supported by configuring any specific ports corresponding to a VLAN. Untagged frames received on the port are classified to the Port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the Port VLAN ID.

Egress tagging can also be configured for a port using Tx Tag field. It can take the following options – *untag_pvid*, *tag_all* and *untag_all*. The default setting is *untag_pvid*.

If *tag_all* is selected all the frames egressing on that port will be tagged.

If *untag_all* is selected, all the frames egressing on the port will be untagged.

If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.

A **MAC-based** VLAN is supported where a VLAN can be configured corresponding to a MAC address.

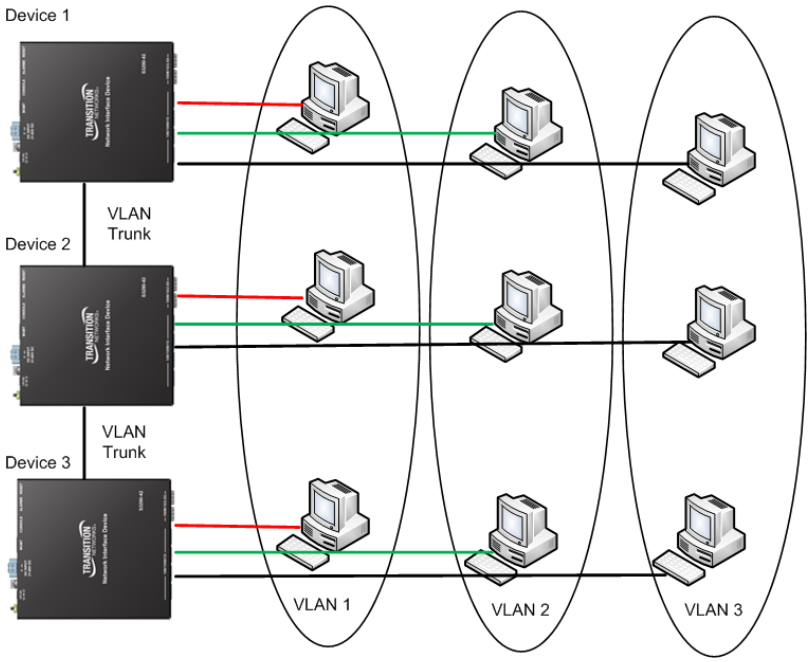
A **Protocol based** VLAN is supported where a VLAN can be configured corresponding to a Protocol group whose Frame type could be any of the following.

1. Ethernet - Valid values for etype ranges from 0x0600-0xffff
2. SNAP - Valid value in this case also is comprised of two different sub values.
   a.OUI: OUI (Organizationally Unique Identifier).
   b. PID: If the OUI is hexadecimal 000000, the protocol 1 ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.
3. LLC - Valid value in this case is comprised of two different sub-values.
   a. DSAP: 1-byte long string (0x00-0xff)
   b. SSAP: 1-byte long string (0x00-0xff)

The precedence of these VLANs is as follows: The MAC-based VLAN is preferred over the Protocol based VLAN and Protocol based VLAN is preferred over Port based VLAN. This will imply that the MAC-based VLAN is preferred over a Port based VLAN.

For the **vlan protocol snap** command, the SNAP OUI = rfc-1042 option enables IETF RFC 1042, which specifies a standard method of encapsulating IP datagrams and Address Resolution Protocol (ARP) requests and replies on IEEE 802 Networks. See https://www.ietf.org/rfc/rfc1042.txt for details.

VLAN Quick Config Example



1. **Add VLAN 2 and 3** (VLAN 1 is created by default):

```
# configure terminal
(config-vlan)# name VLAN2
(config-vlan)# name VLAN3
(config-vlan)#
```

2. **Set access port**; assume that ports 1-3 are connected to the PC. The PVID is different for each port.

```
# config term
(config-if)# switchport access vlan 1
(config-if)# exit
(config)# interface GigabitEthernet 1/2
(config-if)# switchport mode access
(config-if)# switchport access vlan 2
(config-if)# exit
(config)# interface GigabitEthernet 1/3
(config-if)# switchport mode access
(config-if)# switchport access vlan 3
(config-if)#
```

3. **Set access port**; assume port 4 is connected to the other device. Set the allowed VLAN to accept 1-3.

```
(config)# interface GigabitEthernet 1/4
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 1-3
(config-if)#
```

4. **Configure frames** to always be transmitted with a tag on port 4:

```
(config-if)# switchport trunk vlan tag native
(config-if)#
```

Command: Configure Web Privilege Levels

Syntax: **web privilege group** <group_name> level { [configRoPriv <configRoPriv>] [confi gRwPriv <configRwPriv>] [statusRoPriv <statusRoPriv>] [statusRwPriv <statusR wPriv>] }*1

Description: Configure the web privilege level. Enter the new user's level of access to be allowed. This is the privilege level of the user. The valid range is **1** - **15**. If the privilege level value is 15, a user can access all groups (i.e., this user is granted the fully control of the device). But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. The system maintenance (software upload, factory defaults and etc.) requires user privilege level 15. By default, most groups' privilege level 5 has read-only access and privilege level 10 has read-write access. Generally, privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account, and privilege level 5 for a guest account.

Note: this feature only works for web users.

Mode: (config)#

Example: Configure the web privilege levels:

```
(config)# web ?
    privilege    Web privilege
(config)# web??
web privilege group <group_name> level { [ configRoPriv <configRoPriv> ] [ confi
gRwPriv <configRwPriv> ] [ statusRoPriv <statusRoPriv> ] [ statusRwPriv <statusR
wPriv> ] }*1
(config)# web privilege group ?
    <cword>    Valid words are 'Aggregation' 'DDMI' 'DHCP' 'DHCPv6_Client'
               'Debug' 'Diagnostics' 'EPS' 'ERPS' 'ETHER_SAT' 'ETH_LINK_OAM'
               'EVC' 'IP' 'IPMC_Snooping' 'LACP' 'LLDP' 'Loop_Protect'
               'MAC_Table' 'MEP' 'MVR' 'Maintenance' 'NTP' 'PTP' 'Ports'
               'Private_VLANs' 'QoS' 'RMirror' 'Security' 'Spanning_Tree'
               'System' 'UDLD' 'VCL' 'VLAN_Translation' 'VLANs' 'XXRP'
(config)# web privilege group aggr level ?
    configRoPriv    Configuration Read-only level
    configRwPriv    Configuration Read-write level
    statusRoPriv    Status/Statistics Read-only level
    statusRwPriv    Status/Statistics Read-write level
(config)# web privilege group aggr level
(config)# web privilege group xxrp level configRwPriv ?
    <0-15>
(config)# web privilege group xxrp level configRwPriv 15 ?
    configRoPriv    Configuration Read-only level
    statusRoPriv    Status/Statistics Read-only level
    statusRwPriv    Status/Statistics Read-write level
    <cr>
(config)# web privilege group xxrp level configRwPriv 15?
    <0-15>
    <cr>
(config)# web privilege group xxrp level configRwPriv 15?
web privilege group <group_name> level { [ configRoPriv <configRoPriv> ] [ confi
gRwPriv <configRwPriv> ] [ statusRoPriv <statusRoPriv> ] [ statusRwPriv <statusR
wPriv> ] }*1
(config)# web privilege group xxrp level configRwPriv 15?
    <0-15>
    <cr>
(config)# web privilege group xxrp level configRwPriv 15
```

Parameters

Group Name: The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but some groups contain more than one module. Some of these privilege level groups are explained below:

System: e.g., Contact, Name, Location, Timezone, Log.

Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and IP source guard.

IP: Everything except 'ping'.

Port: Everything except 'VeriPHY'.

Diagnostics: 'ping' and 'VeriPHY'.

Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance. Debug is only present in the CLI.

Privilege Levels: Every group has an authorization Privilege level for the following sub groups: Configuration read-only, Configuration/execute read-write, Status/statistics read-only, Status/statistics read-write (e.g., for clearing statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

configRoPriv: (*Configuration Read-only level*) these users are only allowed to monitor status / configuration settings.

configRwPriv: (Configuration Read-write level) these users are only allowed to monitor status and make changes to configuration settings.

statusRoPriv: (Status/Statistics Read-only level) these users are only allowed to monitor status / statistics settings. The privilege level of ‘Read-only’ should be less or equal ‘Read/Write’.

statusRwPriv: Status/Statistics Read-write level (e.g., for clearing statistics).

User Privilege Levels (1-15): The privilege level of the user. The allowed range is 1 to 15.
Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. for clearing of statistics). If the privilege level value is 15, it can access all groups (i.e. it is granted full control of the device). But other 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 the read-write access. The system maintenance functions (software upload, factory defaults, 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** is for a Standard (basic) user account, and
Privilege Level **5** is for a Guest account.

Copy Commands

Command: Copy Config File

Syntax: **copy** { startup-config | running-config | <source_path> } { startup-config | running-config | <destination_path> } [syntax-check]

Description: Copy commands allow transferring or saving the configuration files to and from the switch (copy a config file from source to destination). The TFTP server must be properly configured and running. The parameters are:

<**url_file**> File in FLASH or on TFTP server.
Syntax: <flash:filename | tftp://server/path-and-filename>. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score(_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.
running-config Currently running configuration.
startup-config Startup configuration.

Mode: #

Example:

```
# copy startup-config flash:xxxxx.bin 192.168.1.30
                                      ^
% Invalid word detected at '^' marker.

# copy startup-config flash:xxxxx.bin tftp://192.168.1.30
                                      ^
% Invalid word detected at '^' marker.
# copy startup-config flash ?
    |               Output modifiers
    syntax-check    Perform syntax check on source configuration
    <cr>
# copy startup-config flash | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# copy startup-config f
flash:filename | tftp://server/path-and-filename
<cr>
# copy startup-config flash ?
    |               Output modifiers
    syntax-check    Perform syntax check on source configuration
    <cr>
# copy startup-config flash syntax-check ?
    |       Output modifiers
    <cr>
```

Message: *% Invalid destination syntax, expected flash:filename or tftp://server[:port]/path-to-file*

Example:

```
# copy startup-config f
% Invalid destination syntax, expected flash:filename or
tftp://server[:port]/path-to-file
#
```

Delete Commands

Command: Delete a File

Syntax: **delete** <Path : word> Name of file to delete

Description: Delete one file in the flash: file system.

Mode: *#*

Example: Delete a file from the flash file system.

```
# delete?
    delete    Delete one file in flash: file system
# delete?
delete <path>
# delete ?
    <url_file>    File in FLASH. Sytax: <flash:filename>. A valid file name is
                  a text string drawn from alphabet (A-Za-z), digits (0-9), dot
                  (.), hyphen (-), under score(_). The maximum length is 63 and
                  hyphen must not be first character. The file name content
                  that only contains '.' is not allowed.
```

Dir Commands

Command: Display Directory

Syntax: **dir**

Description: Display directory of all files in the flash: file system.

Mode: *#*

Example:

```
# dir
Directory of flash:
    r- 1970-01-01 00:00:00      312 default-config
    rw 1970-01-01 03:46:35     7913 startup-config
2 files, 8225 bytes total.
# dir ?
    |       Output modifiers
    <cr>
# dir | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# dir |
```

Disable Commands

Command: Disable Priviliged Command Mode

Syntax: **disable** <0-15>

Description: Turn off privileged commands. (The **enable** command turns priv commands back on.)

Mode: #

Example:

```
# disable ?
    <0-15>
    <cr>
# disable?
    disable    Turn off privileged commands
    <cr>
# disable
> enable?
    enable    Turn on privileged commands
    <cr>
> enable ?
    <0-15>    Choose privileged level
    <cr>
> enable
#
```

User EXEC Mode: The User EXEC mode is the initial mode available for the users for the insufficient privileges. The User EXEC mode contains a limited set of commands. The command prompt shown at this level is **>**.

Privileged EXEC Mode: The administrator/user must enter the Privileged EXEC mode in order to have access to the full suite of commands. The Privileged EXEC mode requires password authentication using an 'enable' command if set. The command prompt shown at this level is **#**.

Do Commands

Command: Do (Run Exec Mode Command in Config Mode)

Syntax: **do** <line>

Description: To run exec commands in config mode.

Mode: (config)

Example:

```
# do show ?
    LINE    Exec Command
    <cr>
# do show show
show show
     ^
% Invalid word detected at '^' marker.
(config)# do dir
Directory of flash:
    r- 1970-01-01 00:00:00      304 default-config
    rw 1970-01-01 00:00:10     1013 startup-config
2 files, 1317 bytes total.
(config)#
```

User EXEC Mode: The User EXEC mode is the initial mode available for the users for the insufficient privileges. The User EXEC mode contains a limited set of commands. The command prompt shown at this level is **>**.

Privileged EXEC Mode: The administrator/user must enter the Privileged EXEC mode in order to have access to the full suite of commands. The Privileged EXEC mode requires password authentication using an 'enable' command if set. The command prompt shown at this level is **#**.

Dot1x Commands

Command: Initialize 802.1x Interface

Syntax: **dot1x initialize** [interface <port_type_list>]
dot1x initialize [interface (<port_type> [<plist>])]

Description: IEEE 802.1x is a standard for port-based Network Access Control. It lets you initialize and force an immediate re-authentication.

Mode: #

Example:

```
# dot1x initialize interface ?
    *                    All switches or All ports
    ManagementPort       Management Port
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
# dot1x initialize interface *
    <port_type_list>     List of Port ID, ex, 1/1,3-5;2/2-4,6
# dot1x initialize interface GigabitEthernet ?
    <port_type_list>     Port list in 1/1-6
# dot1x initialize interface 10GigabitEthernet ?
    <port_type_list>     Port list in 1/1-2
# dot1x initialize interface 10GigabitEthernet ?
    <port_type_list>     Port list in 1/1-2
# dot1x initialize interface 10GigabitEthernet 1/2
#
```

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.

In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to “piggy-back” on the successfully authenticated client and gain network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant.

Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance.

Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that will cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

Enable Commands

Command: Enable Priv Command Mode

Syntax: **enable** [<new_priv>]

Description: Turn on privileged commands. (The **disable** command turns priv commands off.)

Mode: >

Example:

```
# enable?
    enable    Turn on privileged commands
    <cr>
# enable ?
    <0-15>    Choose privileged level
    <cr>
# enable?
    enable    Turn on privileged commands
    <cr>
# enable?
enable [ <new_priv> ]
# enable
# enable 15
# show priv
#
```

Multiple S4224 users can be created, identified by the username and Privilege level.

The privilege level of the user allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, that is it will grant the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group.

By default setting, most groups' privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults, etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

The name identifying the privilege group is called the Group name. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contain more than one.

The following description defines these privilege level groups in details:

1. System: Contact, Name, Location, Timezone, Log.
2. Security: Authentication, System Access Management, Port (contains Dot1x port, MAC-based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and IP source guard.
3. IP: Everything except 'ping'.
4. Port: Everything except 'VeriPHY'.
5. Diagnostics: 'ping' and 'VeriPHY'.
6. Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.
7. Debug: Only present in CLI.

Every group has an authorization Privilege level for the following sub groups 1 to 15:

- configuration read-only
- configuration/execute read-write
- status/statistics read-only
- status/statistics read-write (e.g. for clearing of statistics).

User Privilege must be same or greater than the auth Privilege level to have the access to that group.

Exit Commands

Command: Exit EXEC mode

Syntax: **exit**

Description: Exit from EXEC mode or current mode. You must press the Enter key and log back in after.

Mode: #

Example: Exit from EXEC mode and exit current mode:

```
# exit

Press ENTER to get started

Username: admin
Password:
(config)# exit?
    exit    Exit from current mode
    <cr>
(config)# exit??
exit
(config)# exit?
    exit    Exit from current mode
    <cr>
(config)# exit ?
    <cr>
(config)#
```

Firmware Commands

Command: Firmware Swap

Syntax: **firmware swap**

Description: Swap between Active and Alternate firmware image. This may be a version upgrade or downgrade. You must press the Enter key and log back in after the firmware swap completes.

Mode: #

Example: The example below shows a firmware swap.

```
# firmware ?
    swap       Swap between Active and Alternate firmware image.
    upgrade    Firmware upgrade
# firmware swap ?
    <cr>
# firmware swap
... Erase from 0x40fd0000-0x40fdffff: .
... Program from 0x87ff0000-0x88000000 to 0x40fd0000: .
... Program from 0x87ff000a-0x87ff000c to 0x40fd000a: .
Alternate image activated, now rebooting.
# +M25PXX : Init device with JEDEC ID 0x20BA18.
S4224 board detected (VSC7460 Rev. B).

RedBoot(tm) bootstrap and debug environment [ROMRAM]
Non-certified release, version 1_15-TN - built 20:05:49, Jul 31 2013

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) JAGUAR
RAM: 0x80000000-0x88000000 [0x80021f08-0x87fe1000 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 0x80040000-0x80ef4660
RedBoot> go

Press ENTER to gW snmp 00:00:09 45/vtss_snmp_mibs_init#5774: Warning: Fix tnSync
eMIB.c - enable in s4224.mk
et startedtimeout set failed% Error in file startup-config, line 334:
ethersat collector enabled
                   ^
% Invalid word detected at '^' marker.

Profile number 1 and name "SatTest1"
% 1 problem found during configuration.


Username:
```

Command: Firmware Upgrade

Syntax: **firmware upgrade** <tftpserver_path_file> [activate { now | defer }]

TFTP Server IP address, path and file name for the server containing the new image.
<**word**> [activate { now | defer }]
defer Defer activation until later. Swap the image to the activate bank to activate. (default)
now Activate the image now.

Description: Upgrade the device firmware. **Warning**: after starting flash update - do not power off device! While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. **Note**: It is a good idea to create a backup of the configuration before upgrading the firmware. The S4224 IP address is reset to default values during a firmware upgrade.

Mode: #

Example: Show the device firmware upgrade functions and performa an upgrade:

```
# firmware upgrade 172.16.45.41 ?
    activate    Select when the image will be activated.
    <cr>
# firmware upgrade 172.16.45.41 activate ?
    defer    Defer activation until later. Swap the image to the activate bank to activate.
             (default)
    now      Activate the image now.
# firmware upgrade 172.16.45.41 activate now ?
    <cr>
# firmware upgrade 172.16.45.41 activate now
% 172.16.45.41 is an invalid TFTP path - Expecting something like
tftp://10.10.10.10/path/new_image.dat
# firmware upgrade 172.16.45.41 activate defer
% 172.16.45.41 is an invalid TFTP path - Expecting something like
tftp://10.10.10.10/path/new_image.dat
# firmware upgrade tftp://192.186.1.110 activate defer
#

# firmware upgrade tftp://192.168.1.30/c://TFTP-Root
Download of /c://TFTP-Root from 192.168.1.30 failed: Access violation.
# $e tftp://192.168.1.30/c://TFTP-RootS4224-base-vtss-v3.6x.dat
Download of /c://TFTP-RootS4224-base-vtss-v3.6x.dat from 192.168.1.30 failed:
 Access violation.
#
# firmware upgrade tftp://192.168.1.30 ?
    activate    Select when the image will be activated.
    <cr>
# firmware upgrade tftp://192.168.1.30 activate ?
    defer    Defer activation until later. Swap the image to the activate bank
             to activate. (default)
    now      Activate the image now.
# firmware upgrade tftp://192.168.1.30 activate now ?
    <cr>
# firmware upgrade tftp://192.168.1.30 activate now
#
```

CLI Commands to Regain Access to the Web GUI

Anytime the IP Address shows as blank or DOWN (e.g., after a Software Upload), you can use the following CLI commands to regain web GUI access:

```
# show ip int brief
Vlan Address              Method   Status
---- -------------------- -------- ------
# conf term
(config)# int vlan 1
(config-if-vlan)# ip addr 192.168.1.110 255.255.255.0
(config-if-vlan)# end
# show ip int brief
Vlan Address              Method   Status
---- -------------------- -------- ------
   1 192.168.1.110/24     Manual   UP
#
```

You can then access the web GUI via the IP address and netmask entered (e.g., 192.168.1.110 and 255.255.255.0 in the example above). See the S4224 CLI Reference manual for details.

Help Commands

Command: Help

Syntax: **help**

Description: Description of the interactive help system.

Mode: #

Example: Display the help file:

```
# help
Help may be requested at any point in a command by entering a
question mark '?'.  If nothing matches, the help list will be
empty and you must backup until entering a '?' shows the
available options. Two styles of help are provided:
1. Full help is available when you are ready to enter a
    command argument (e.g. 'show ?') and describes each
    possible argument.
2. Partial help is provided when an abbreviated argument is
    entered and you want to know what arguments match the input
    (e.g. 'show pr?'.)

#
```

IPv4 Commands

Command: IP v4 DHCP Command

Syntax: **ip dhcp retry interface vlan** <vlan_id>

Description: IPv4 command used to restart the DHCP query process.

Mode: #

Example:

```
# ip ?
    dhcp    Dhcp commands
# ip dhcp ?
    retry    Restart the DHCP query process
# ip dhcp
retry
# ip dhcp retry ?
    interface    Interface
# ip dhcp retry interface ?
    vlan    Vlan interface
# ip dhcp retry interface vlan ?
    <vlan_id>    Vlan ID
# ip dhcp retry interface vlan 10
% Failed to restart DHCP client on VLAN = 10.
# ip dhcp retry interface vlan 1
#
```

Message: "*Failed to restart DHCP client on VLAN = x.*" displays if specified VLAN does not exist.

Recovery: 1. Create a VLAN or specify another VID (VLAN ID).

Related commands: `(config)# ip dhcp`

IPv6 Commands

Command: IP v6 DHCP Command

Syntax: **ipv6 dhcp-client restart** [interface vlan <v_vlan_list>]

Description: The IPv6 command is used to restart the DHCPv6 client service. The Dynamic Host Configuration Protocol for IPv6 (DHCP) enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility. See IETF RFC 3315 for more information. The parameters are:

<***vlan_list***> : The VLANs associated with the IP interface. Only ports in this VLAN are able to access the IP interface.

Mode: #

```
# ipv6 ?
    dhcp-client    Manage DHCPv6 client service
# ipv6 dhcp-client ?
    restart    Retart DHCPv6 client service
# ipv6 dhcp-client restart ?
    interface    Select an interface to configure
    <cr>
# ipv6 dhcp-client restart interface ?
    vlan    VLAN of IPv6 interface
# ipv6 dhcp-client restart interface vlan ?
    <vlan_list>    IPv6 interface VLAN list
# ipv6 dhcp-client restart interface vlan 1
```

Messages:

W web 01:09:15 75/handler_ip_config#435: Warning: Operation failed: Address conflict
Press ENTER to get started

% Invalid DHCPv6 client interface Vlan1

Link OAM Commands

Command: Link OAM Remote Loopback Config

Syntax: **link-oam remote-loopback** { start | stop } interface (<port_type> [<v_port_type_list>])

{ **start** | **stop** } initiate or end the loopback test. Start/Stop remote LB test on specified interface(s). The interfaces to specify are:

*****	All switches or All ports
ManagementPort	Management Port
GigabitEthernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port

Description: Configure remote loopback on one or more interfaces.

Mode: #

Example: Configure remote loopback:

```
# link-oam remote-loopback start ?
    interface    Start/Stop remote loopback test on a specific interface or interfaces.
# link-oam remote-loopback start interface ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
# link-oam remote-loopback start interface g ?
    PORT_LIST    Port list in 1/1-6
# link-oam remote-loopback start interface 10GigabitEthernet ?
    PORT_LIST    Port list in 1/1-2
# link-oam remote-loopback stop interface ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
# link-oam remote-loopback stop interface *
% Requested configuration is not supported with the current OAM mode
# link-oam remote-loopback stop interface g ?
    PORT_LIST    Port list in 1/1-6
# link-oam remote-loopback stop interface g 1/1-4
% Requested configuration is not supported with the current OAM mode for Gigabit Ethernet 1/1
#
```

Messages: *No such port: GigabitEthernet 2/1*

Requested configuration is not supported with the current OAM mode for xxxx

*% No valid port in wildcard, * 1/7*

Logout Commands

Command: Logout (Exit EXEC mode)

Syntax: **logout**

Description: Exit from EXEC mode. You must the log back in.

Mode: #

Example:

```
# logout?
logout
# logout

Press ENTER to get started

Username: admin
Password:
#
```

More (Display) Commands

Command: more

Syntax: **more** <Path> File in FLASH or on TFTP server .

Description: Display file in FLASH or on TFTP server.

Mode: #

Example:

```
# more ?
    <url_file>    File in FLASH or on TFTP server. Sytax: <flash:filename |
                  tftp://server/path-and-filename>. A valid file name is a text
                  string drawn from alphabet (A-Za-z), digits (0-9), dot (.),
                  hyphen (-), under score(_). The maximum length is 63 and
                  hyphen must not be first character. The file name content
                  that only contains '.' is not allowed.
# more?
    more    Display file
#
```

Messages: *% Invalid source syntax, expected flash:filename or tftp://server[:port]/path-to-file*

No Commands

It is possible to either remove specific configuration or reset it to its default values. In the general case, almost each configuration command has a corresponding 'no' form. The 'no' form is syntactically similar (but not necessarily identical) to the configuration command, but either resets the parameters to defaults for the configurable item being addressed, or removes the item altogether. In many cases 'no' can be read as "no(t) different from default settings".

Command: No (Negate a Command or Set its Defaults)

Syntax: **no debug prompt** : Clear prompt for testing

no port-security shutdown [interface <port_type_list>] : Reopen one or more ports whose limit is exceeded and is shut down. No Port security (psec limit).

editing Enable command line editing

exec-timeout : Set the EXEC timeout.

history : Control the command history function.

length : Set number of lines on a screen.

width : Set width of the display terminal.

Description: Every configuration command has a "no" form to negate or set its default. In general, the no form is used to reverse the action of a command or reset a value back to the default. For example, the '**no ip routing**' configuration command reverses the '**ip routing'** of an interface.

Mode: # and (config)#

Example: The **no** command in # mode:

```
# n?
    no    Negate a command or set its defaults
# no ?
    debug            Debugging functions
    port-security    Port security (psec limit)
    ptp              Misc non persistent 1588 settings.
    terminal         Set terminal line parameters
# no debug ?
    interrupt-monitor    Print out of reception of the selected interrupt
                         source.
    ipv6                 IPv6 configuration commands
    trace                No debug trace hunt
# no debug i
interrupt-monitor  ipv6
# no debug interrupt-monitor ?
    source    The selected interrupt source.
# no debug interrupt-monitor source ?
    <uint>    The possible values are enum vtss_interrupt_source_t values found
              in file board/interrupt_api.h
# no debug interrupt-monitor source 11
# no debug ipv6 ?
    nd    IPv6 Neighbor Discovery debugging
# no debug ipv6 nd ?
    <cr>
# no debug ipv6 nd
  IPv6 Neighbor Discovery events debugging is off
# no port-security ?
    shutdown    Reopen one or more ports whose limit is exceeded and shut down.
# no port-security shutdown ?
```

```
    interface
    <cr>
# no port-security shutdown interface ?
    *                    All switches or All ports
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
# no ptp ?
    <0-3>    Clock instance [0-3]
# no ptp 0 ?
    wireless    Enable wireless mode for one or more interfaces.
# no ptp 0 wireless ?
    mode    Enable wireless mode for an interface.
# no ptp 0 wireless mode ?
    interface    Interface
# no ptp 0 wireless mode interface ?
    *                    All switches or All ports
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
# no terminal ?
    editing         Enable command line editing
    exec-timeout    Set the EXEC timeout
    history         Control the command history function
    length          Set number of lines on a screen
    width           Set width of the display terminal
# no terminal
```

Example: The **no** command in (config)# mode:

```
(config)# no ?
    aaa              Authentication, Authorization and Accounting
    access           Access management
    access-list      Access list
    aggregation      Aggregation mode
    banner           Define a login banner
    clock            Configure time-of-day clock
    ddmi             DDMI Information
    debug            Debugging functions
    dot1x            IEEE Standard for port-based Network Access Control
    enable           Modify enable password parameters
    eps              Ethernet Protection Switching.
    erps             Ethernet Ring Protection Switching
    evc              Ethernet Virtual Connections
    gvrp             Enable GVRP feature
    hostname         Set system's network name
    interface        Select an interface to configure
    ip               Internet Protocol
    ipmc             IPv4/IPv6 multicast configuration
    ipv6             IPv6 configuration commands
    ipv6             IPv6 configuration commands
    lldp             LLDP configurations.
    logging          System logging message
    loop-protect     Loop protection configuration
    mac              MAC table entries/configuration
    mep              Maintenance Entity Point
    monitor          Monitoring different system events
    mvr              Multicast VLAN Registration configuration
    network-clock    network-clock
    ntp              Configure NTP
```

```
    port-security    Enable/disable port security globally.
    privilege        Command privilege parameters
    ptp
    qos              Quality of Service
    radius-server    Configure RADIUS
    rmon             Remote Monitoring
    snmp-server      Enable SNMP server
    spanning-tree    STP Bridge
    switchport       vlan - VLAN translation
    tacacs-server    Configure TACACS+
    udld             Disable UDLD configurations on all fiber-optic ports.
    username         Establish User Name Authentication
    vlan             Vlan commands
    web              Web
(config)# no
```

Ping Commands

Command: ping

Mode: #

Syntax: **ping ip** { <v_ip_addr> | <v_ip_name> } [repeat <count>] [size <size>] [interval <seconds>]
ping ipv6 { <v_ipv6_addr> | <v_ipv6_name> } [repeat <count>] [size <size>] [interval <seconds>] [interface vlan <v_vlan_id>]

Description: Send ICMP echo messages in IPv4 or IPv6.

Example: View the ping command options and run a successful ipv4 **ping**:

```
# ping ?
    ip      IP (ICMP) echo
    ipv6    IPv6 (ICMPv6) echo
# ping?
    ping    Send ICMP echo messages
# ping?
ping ip { <v_ip_addr> | <v_ip_name> } [ repeat <count> ] [ size <size> ] [ inter
val <seconds> ]
ping ipv6 { <v_ipv6_addr> | <v_ipv6_name> } [ repeat <count> ] [ size <size> ] [
 interval <seconds> ] [ interface vlan <v_vlan_id> ]
# ping ip 192.168.1.110 interval 10 repeat 10 size 10
PING server 192.168.1.110, 10 bytes of data.
18 bytes from 192.168.1.110: icmp_seq=0, time=0ms
18 bytes from 192.168.1.110: icmp_seq=1, time=0ms
18 bytes from 192.168.1.110: icmp_seq=2, time=0ms
18 bytes from 192.168.1.110: icmp_seq=3, time=0ms
18 bytes from 192.168.1.110: icmp_seq=4, time=0ms
18 bytes from 192.168.1.110: icmp_seq=5, time=0ms
18 bytes from 192.168.1.110: icmp_seq=6, time=0ms
18 bytes from 192.168.1.110: icmp_seq=7, time=0ms
18 bytes from 192.168.1.110: icmp_seq=8, time=0ms
18 bytes from 192.168.1.110: icmp_seq=9, time=0ms
Sent 10 packets, received 10 OK, 0 bad
#
```

Messages:

% Please specify correct egress IPv6 interface.
sendto: Network is down

A full IPv6 address (e.g., **FE80:0000:0000:0000:0202:B3FF:FE1E:8329**) shows a 128-bit address in eight 16-bit blocks in the format global:subnet:interface.

A collapsed IPv6 address (e.g., **FE80::0202:B3FF:FE1E:8329**): the **::** (consecutive colons) notation can be used to represent four successive 16-bit blocks that contain zeros. When SAS software encounters a collapsed IP address, it reconstitutes the address to the required 128-bit address in eight 16-bit blocks.

A port number (e.g., **[2001:db8:0:1]:80**): the brackets are necessary only if also specifying a port number. Brackets are used to separate the address from the port number. If no port number is used, the brackets can be omitted.

An IP address containing a URL: **http://[2001:db8:0:1]:80** - the **http://** prefix specifies a URL. The brackets are necessary only if also specifying a port number. Brackets are used to separate the address from the port number. If no port number is used, the brackets can be omitted.

PTP Commands

Command: Configure PTP Local Clock and Wireless Delay

Mode: #

Syntax: **ptp** <clockinst> **local-clock** { update | ratio <ratio> }
ptp <clockinst> **wireless delay** <base_delay> [<incr_delay>] interface (<port_type> [<v_port_type_list>])
ptp <clockinst> **wireless mode interface** (<port_type> [<v_port_type_list>])
ptp <clockinst> **wireless pre-notification interface** (<port_type> [<v_port_type_list>])

Description: Configure Precision Timing Protocol. Configure the IEEE 1588 PTP parameters (miscellaneous non-persistent 1588 settings). PTP (IEEE 1588-2008 or 3 version 2) technology is used for distribution of frequency and time of day (ToD).

Example: Show the various **ptp** commands available in exec mode.

```
# ptp?
    ptp    Misc non persistent 1588 settings
# ptp ?
    <0-3>    PTP Clock instance [0-3]
# ptp??
ptp <clockinst> local-clock { update | ratio <ratio> }
ptp <clockinst> wireless delay <base_delay> [ <incr_delay> ] interface ( <port_type> [
<v_port_type_list> ] )
ptp <clockinst> wireless mode interface ( <port_type> [ <v_port_type_list> ] )
ptp <clockinst> wireless pre-notification interface ( <port_type> [ <v_port_type_list> ] )
# ptp 0 ?
    local-clock    Update local clock current time, or set clock ratio
    wireless       Enable wireless mode for one or more interfaces.
# ptp 0 local-clock ?
    ratio     Set the local master clock frequency ratio.
    update    The local clock is synchronized to the eCos system clock
# ptp 0 local-clock ratio ?
    <-10000000-10000000>    Ratio in units of 0,1 PPB, (ratio > 0 => faster
                            clock, ratio < 0 => slower clock).
# ptp 0 local-clock ratio 200 ?
    <cr>
# ptp 0 local-clock ratio 200
# ptp 0 wireless ?
    delay
    mode                Enable wireless mode for an interface.
    pre-notification    Issue a pre notification that the wireless modem is going to change.
# ptp 0 wireless delay ?
    <0-1000000000>    Base wireless transmission delay (in picco seconds)
# ptp 0 wireless mode ?
    interface    Interface
# ptp 0 wireless mode interface ?
    *                    All switches or All ports
    ManagementPort       Management Port
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
# ptp 0 wireless pre-notification ?
    interface
# ptp 0 wireless pre-notification interface ?
    *                    All switches or All ports
    ManagementPort       Management Port
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
```

Related commands: <config># **ptp** and # **show ptp**

Messages: *Wireless mode not available for ptp instance 0, port 2*

Reload Commands

***Command*: reload**

Mode: #

Syntax: **reload** { { { cold | warm } [sid <usid>] } | { defaults [keep-ip] } }

cold Reload cold. You must log in again when done.
defaults Reload defaults without rebooting; try to keep default VLAN 1 IP address .

Description: Reload the S4224. You must log in again when the command completes. The reload Command provides two “restart” options. The "reload cold" command actually performs a warm reboot.

Example: Run the commands and display resulting information.

```
# reload defaults keep-ip
% Reloading defaults, attempting to keep VLAN 1 IP address. Please stand by.
% Reloading defaults complete.
# reload cold
% Cold reload in progress, please stand by.
# +M25PXX : Init device with JEDEC ID 0xEF4018.
S4224 board detected (VSC7428 Rev. B).

RedBoot(tm) bootstrap and debug environment [ROMRAM]
Non-certified release, version 1_12-TN - built 12:04:49, May  7 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 0x80040000-0x8091e4f8
RedBoot> go
E main 00:00:00 30/dumpbuffer_init#197: Error: Bootloader unable to keep fault data. Please upgrade
bootloader!
Version      : S4224 (standalone) 2..2.0
Build Date   : 2014-01-15T21:13:11-06:00
Warning: Return addresses are highly unreliable (code seems to be compiled with-O2)
ID  State SetPrio CurPrio Name                   1sec Load 10sec Load Stack Base Size  Used
--- ----- ------- ------- ---------------------- --------- ---------- ---------- ----- -----
DSR N/A       N/A     N/A DSR Context                 N/A        N/A        N/A   N/A   N/A
 30 Run         7       7 Init Modules               N/A        N/A 0x81c77850 16384  1720*
#0  0x800774a0
#1  0x803ff91c
#2  0x800774a0
#3  0x8040623c
#4  0x803545d0
#5  0x8033c9d0
#6  0x8024ccb8
#7  0x8024b854
#8  0x80293ee4
#9  0x8040223c
#10 0x80402210
Press ENTER to get started
```

Note: If you run "reload defaults" and then "reload cold", after reboot, the result is an IP address of 192.168.0.1 on vlan 1 after ~70 seconds of uptime.

Send Commands

Command: Send a Message

Syntax: **send** { * | <0~16> | console 0 | vty <0~15> } <line128>

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

***** All tty lines.

<**0**~**16**> Send a message to multiple lines.

console Primary terminal line.

vty Virtual terminal.

Description: Send a message to other tty lines. Enter a TEXT message; end with the character '**w**'.

Mode: #

Example:

```
# send * GGGGG

----------------------------------------
*** Message from line 0:

----------------------------------------
#
# send ?
    *          All tty lines
    <0~16>     Send a message to multiple lines
    console    Primary terminal line
    vty        Virtual terminal
# send * ?
    LINE    Message to be sent to lines, in 128 char's
# send * I am back. ?
    LINE    Message to be sent to lines, in 128 char's
    <cr>
# send * I am back.
Enter TEXT message.  End with the character 'I'.
I I am back.

----------------------------------------
*** Message from line 0:
 am back.

----------------------------------------
#
```

Show Commands

Use the **show** command to display current device configuration, statistics, and other information. The family of 'show' commands is the cornerstone of CLI-based system monitoring. Most features implement one or more 'show' commands that will display a relevant mix of status and configuration. The 'show' commands exist only in the two Exec modes and are subject to session privilege level enforcement. Therefore, listing the largest possible set of 'show' commands requires the session to be at level 15.
Note: The exact set of available commands, parameters and output format depends on the system configuration and software version, so some of the following commands and examples may not be applicable to all systems.

```
# show?
    show    Show running system information
# show ?
    aaa               Authentication, Authorization and Accounting methods
    access            Access management
    access-list       Access list
    aggregation       Aggregation port configuration
    clock             Configure time-of-day clock
    ddmi              DDMI configuration
    dot1x             IEEE Standard for port-based Network Access Control
    eps               Ethernet Protection Switching
    erps              Ethernet Ring Protection Switching
    ethersat          ethersat (Service Activation Test)
    evc               Ethernet Virtual Connections
    green-ethernet    Green ethernet (Power reduction)
    history           Display the session command history
    interface         Interface status and configuration
    ip                Internet Protocol
    ipmc              IPv4/IPv6 multicast configuration
    ipv6              IPv6 configuration commands
    lacp              LACP configuration/status
    line              TTY line information
    link-oam          Link OAM configuration
    lldp              Display LLDP neighbors information.
    logging           System logging message
    loop-protect      Loop protection configuration
    mac               Mac Address Table information
    mep               Maintenance Entity Point
    monitor           Monitoring different system events
    mvr               Multicast VLAN Registration configuration
    network-clock     Show selector state.
    ntp               Configure NTP
    ntp               Configure NTP
    port-security     Port Security status - Port Security is a module with no
                      direct configuration.
    privilege         Display command privilege
    process           process
    ptp               Precision time Protocol (1588)
    pvlan             PVLAN configuration
    qos               Quality of Service
    radius-server     RADIUS configuration
    rmon              RMON statistics
    running-config    Show running system information
    snmp              Display SNMP configurations
    spanning-tree     STP Bridge
    switchport        Display switching mode characteristics
    system            system
    tacacs-server     TACACS+ configuration
    terminal          Display terminal configuration parameters
```

```
    udld              Uni Directional Link Detection(UDLD) configurations,
                      statistics and status
    user-privilege    Users privilege configuration
    users             Display information about terminal lines
    version           System hardware and software status
    vlan              VLAN status
    web               Web
# show
```

The **show** commands are described in the following sections.

Command: Show Login Methods (AAA)

Syntax: **show aaa**
Description: Display the current Authentication, Authorization and Accounting methods Login methods and Output modifiers.
Mode: #
Example: Display the current AAA Login methods:

```
# show aaa?
    aaa     Login methods
    <cr>
# show aaa ?
    |       Output modifiers
    <cr>
# show aaa
Authentication :
  console : local
  telnet  : local
  ssh     : local
  http    : local
Authorization :
  console : no, commands disabled
  telnet  : no, commands disabled
  ssh     : no, commands disabled
Accounting :
  console : no, commands disabled, exec disabled
  telnet  : no, commands disabled, exec disabled
  ssh     : no, commands disabled, exec disabled
# show aaa | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show aaa |
```

Command: Show Access List

Syntax: **show access-list** [interface [<port_type_list>]] [rate-limiter [<1~16>]] [ace statistics [<1~256>]]

Description: Display the current Access List parameters.

Mode: #

Example:

```
# show access-list ?
    |               Output modifiers
    ace             Access list entry
    ace-status      The local ACEs status
    interface       Select an interface to configure
    rate-limiter    Rate limiter
    <cr>
# show access-list

Switch access-list ace number: 0

Switch access-list rate limiter ID 1 is 1 pps
Switch access-list rate limiter ID 2 is 1 pps
Switch access-list rate limiter ID 3 is 1 pps
Switch access-list rate limiter ID 4 is 1 pps
Switch access-list rate limiter ID 5 is 1 pps
Switch access-list rate limiter ID 6 is 1 pps
Switch access-list rate limiter ID 7 is 1 pps
Switch access-list rate limiter ID 8 is 1 pps
Switch access-list rate limiter ID 9 is 1 pps
Switch access-list rate limiter ID 10 is 1 pps
Switch access-list rate limiter ID 11 is 1 pps
Switch access-list rate limiter ID 12 is 1 pps
Switch access-list rate limiter ID 13 is 1 pps
Switch access-list rate limiter ID 14 is 1 pps
Switch access-list rate limiter ID 15 is 1 pps
Switch access-list rate limiter ID 16 is 1 pps

ManagementPort 1/1 :
--------------------
  action is permit
  policy ID is 0
  rate limiter ID is disabled
  redirect is disabled
  logging is disabled
  shutdown is disabled
  port-state is enabled
  counter is 138

GigabitEthernet 1/1 :
---------------------
  action is permit
  policy ID is 0
  rate limiter ID is disabled
  redirect is disabled
  logging is disabled
  shutdown is disabled
  port-state is enabled
  counter is 3083

GigabitEthernet 1/2 :
---------------------
  action is permit
-- more --, next page: Space, continue: g, quit: ^C
```

Command: Show Access Management Config

Syntax: **show access management**

Description: Display the current Access Management state and output modifiers. The maximum Access Management filter entries allowed is 16. If the application's type matches any one of the access management entries, it will allow access to the switch.

- <***1***~***16***> : ID of access management entry
- **|** : Output modifiers
- ***statistics*** : Statistics data
- <cr>

Mode: #

Example 1: Display the current Access Management mode and statistics:

```
# show access management ?
    <1~16>        ID of access management entry
    |             Output modifiers
    statistics    Statistics data
    <cr>
# show access management<cr>
Switch access management mode is disabled

W: WEB/HTTPS
S: SNMP
T: TELNET/SSH

Idx VID  Start IP Address                End IP Address                W S T
--- ---  ------------------------------ ------------------------------ - - -
# show access management 1
Switch access management mode is disabled

W: WEB/HTTPS
S: SNMP
T: TELNET/SSH

Idx VID  Start IP Address                End IP Address                W S T
--- ---  ------------------------------ ------------------------------ - - -
# show access management statistics

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

Command: Show Access Control List ACE Status

Syntax: **show access-list ace-status** [static] [link-oam] [loop-protect] [dhcp] [ptp] [upnp] [arp-inspection] [evc] [mep] [ipmc] [ip-source-guard] [ip-mgmt] [conflicts] [switch <switch_list>]

Description: Display the current Access List ACE Status. Shows the ACEs that did not get applied to the hardware due to hardware limitations.

The Access Control List consists of a table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

The ACE will only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. There can be 16 different ACL rate limiters. A Rate Limiter ID could be assigned to the ACE(s) or to the ingress port(s).

An ACE consists of several parameters. These parameters vary according to the frame type selected. The ingress port must be selected for the ACE, and then the frame type. Different parameter options are displayed depending on the frame type selected.

Note that:

- additional MAC and EtherType parameters are available for ACE configuration when the Frame Type chosen is ‘EtherType’ match.
- additional MAC and ARP parameters are available for ACE configuration when the Frame Type is chosen as ‘ARP’ match.
- additional MAC and ARP parameters are available for ACE configuration when the Frame Type is chosen as ‘IP’ match.
- additional parameters are available for config when the IP Protocol Filter is selected as ICMP.
- additional parameters are available for config when the IP Protocol Filter is selected as UDP.
- additional parameters are available for config when the IP Protocol Filter is selected as TCP.

Mode: #

Example 1: Display the ACE status.

```
# show access-list ace-status?
    ace-status    The local ACEs status
    <cr>
# show access-list ace-status
User
----
S   : static
?   : ipManagement
IPSG: ipSourceGuard
IPMC: ipmc
EVC: evc
MEP : mep
ARPI: arpInspection
?   : upnp
PTP : ptp
DHCP: dhcp
LOOP: loopProtect
?   : ttLoop
?   : y1564
?   : ethersat
LOAM: linkOam
?   : ztp
```

```
User ID   Frame  Action Rate L.  CPU    Counter Conflict
---- --   -----  ------ -------- ------ ------- --------
PTP  1    EType  Deny   Disabled Yes        427 No
PTP  2    EType  Deny   Disabled Yes          0 No
PTP  4    EType  Deny   Disabled Yes          0 No
PTP  3    EType  Deny   Disabled Yes          0 No
MEP  3    EType  Deny   Disabled No (0)       0 No
MEP  2    EType  Deny   Disabled No (0)       0 No
MEP  1    EType  Permit Disabled Yes          0 No
Switch 1 access-list ace number: 7
#

# show access-list ace-status ?
    |                  Output modifiers
    arp-inspection     The ACEs that are configured by ARP Inspection module
    conflicts          The ACEs that did not get applied to the hardware due to hardware
                       limitations
    dhcp               The ACEs that are configured by DHCP module
    evc                The ACEs that are configured by EVC module
    ip-source-guard    The ACEs that are configured by IP Source Guard module
    ipmc               The ACEs that are configured by IPMC module
    link-oam           The ACEs that are configured by Link OAM module
    loop-protect       The ACEs that are configured by Loop Protect module
    mep                The ACEs that are configured by MEP module
    ptp                The ACEs that are configured by PTP module
    static             The ACEs that are configured by users manually
    <cr>
```

Example 2: Display the ACEs' status.

```
# show access-list ace-status
User
----
S   : Static
IPSG: IP Source Guard
IPMC: IPMC
EVC: EVC
MEP : MEP
ARPI: ARP Inspection
PTP : PTP
DHCP: DHCP
LOOP: Loop Protect
LOAM: Link OAM

User ID   Frame  Action Rate L.  Mirror   CPU    Counter Conflict
---- --   -----  ------ -------- -------- ------ ------- -------
DHCP 1    UDP    Deny   Disabled Disabled Yes          0 No
DHCP 2    UDP    Deny   Disabled Disabled Yes          0 No
MEP  6    EType  Filter Disabled Disabled No (0)       0 No
MEP  4    EType  Filter Disabled Disabled No (0)       0 No
MEP  1    EType  Deny   Disabled Disabled No (0)       0 No
MEP  2    EType  Deny   Disabled Disabled Yes          0 No
MEP  3    EType  Deny   Disabled Disabled Yes          0 No
MEP  5    EType  Deny   Disabled Disabled Yes          0 No
S    1    EType  Filter 1        Enabled  No           0 No
Switch 1 access-list ace number: 9
#
```

Example 3: Display the ACE conflicts status.

```
# show access-list ace-status conflicts
User
----
S   : static
?   : ipManagement
IPSG: ipSourceGuard
IPMC: ipmc
EVC: evc
MEP : mep
ARPI: arpInspection
?   : upnp
PTP : ptp
DHCP: dhcp
LOOP: loopProtect
?   : ttLoop
?   : y1564
LOAM: linkOam
?   : ztp
Switch 1 access-list ace number: 0
#
```

Example 4: Display the status of the other ACE status functions:

```
# show access-list ace-status | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show access-list ace-status arp-inspection
Switch 1 access-list ace number: 0
# show access-list ace-status dhcp
Switch 1 access-list ace number: 0 # show access-list ace-status evc
Switch 1 access-list ace number: 0
# show access-list ace-status ip-source-guard
Switch 1 access-list ace number: 0
# show access-list ace-status ipmc
Switch 1 access-list ace number: 0
# show access-list ace-status link-oam
Switch 1 access-list ace number: 0
# show access-list ace-status loop-protect
Switch 1 access-list ace number: 0
# show access-list ace-status arp-inspection evc
User
----
S   : static
?   : ipManagement
IPSG: ipSourceGuard
IPMC: ipmc
EVC: evc
MEP : mep
ARPI: arpInspection
?   : upnp
PTP : ptp
DHCP: dhcp
LOOP: loopProtect
?   : ttLoop
?   : y1564
LOAM: linkOam
```

```
?   : ztp

User ID   Frame  Action Rate L.  Mirror   CPU    Counter Conflict
---- --   -----  ------ -------- -------- ------ ------- -------
EVC  501  LLC    Deny   Disabled Disabled Yes          0 No
EVC  499  EType  Deny   Disabled Disabled Yes          0 No
Switch 1 access-list ace number: 2
```

Example 5: Display the status of the other ACE status MEP:

```
# show access-list ace-status mep
User
----
S   : static
?   : ipManagement
IPSG: ipSourceGuard
IPMC: ipmc
EVC: evc
MEP : mep
ARPI: arpInspection
?   : upnp
PTP : ptp
DHCP: dhcp
LOOP: loopProtect
?   : ttLoop
?   : y1564
?   : ethersat
LOAM: linkOam
?   : ztp

User ID   Frame  Action Rate L.  Mirror   CPU    Counter Conflict
---- --   -----  ------ -------- -------- ------ ------- -------
MEP  2    EType  Filter Disabled Disabled No (O)       0 No
MEP  1    EType  Filter Disabled Disabled No (O)       0 No
MEP  3    EType  Deny   Disabled Disabled Yes          0 No
MEP  4    EType  Deny   Disabled Disabled No (O)       0 No
MEP  5    EType  Deny   Disabled Disabled Yes          0 No
MEP  6    EType  Deny   Disabled Disabled Yes          0 No
Switch 1 access-list ace number: 6
# show access-list ace-status arp-inspection
Switch 1 access-list ace number: 0
```

Command: Show Aggregation Port Configuration

Syntax: **show aggregation mode**

Description: Display the current aggregation mode and port configuration. Displays the Traffic distribution mode information.

Mode: #

Example: Display the current aggregation mode and port configuration:

```
# show aggregation mode
Aggregation Mode:

SMAC  : Enabled
DMAC  : Disabled
IP    : Enabled
Port  : Enabled
# show aggregation mode ?
    |       Output modifiers
    <cr>
# show aggregation mode | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show aggregation mode |

# show aggregation ?
    |       Output modifiers
    mode    Traffic distribution mode
    <cr>
# show aggregation
Aggr ID  Name    Type    Speed     Configured Ports                              Aggregated Ports
-------  ------  ------  --------  --------------------------------------------- ----------------
1        LLAG1   Static  Undefined GigabitEthernet 1/2 10GigabitEthernet 1/1-2   none

#
```

Command: Show Clock Configuration

Syntax: **show clock**
show clock detail

Description: Display the current time-of-day clock configuration and/or related DST and Time zone details.

Mode: #

Example:

```
# show clock?
    clock    Configure time-of-day clock
    <cr>
# show clock detail
System Time     : 1970-01-01T00:57:12+00:00

Timezone : Timezone Offset : 0 ( 0 minutes)
Timezone Acronym :

Daylight Saving Time Mode : Disabled.
Daylight Saving Time Start Time Settings :
        Week: 1
        Day: 1
        Month: 1
        Date: 1
        Year: 2014
        Hour: 0
        Minute: 0
Daylight Saving Time End Time Settings :
        Week: 1
        Day: 1
        Month: 1
        Date: 1
        Year: 2097
        Hour: 0
        Minute: 0
Daylight Saving Time Offset : 1 (minutes)
#
```

Command: Show DDMI State

Syntax: **show ddmi**

Description: Display the current DDMI (Digital Diagnostics Monitoring Interface) state. DDMI provides an enhanced digital diagnostic monitoring interface for optical transceivers which allows real time access to device operating parameters.

Mode: #

Example:

```
# show ddmi?
    ddmi    DDMI configuration
    <cr>
# show ddmi ?
    <cr>
# show ddmi
Current mode: Enabled
#
```

Command: Show dot1x (IEEE 802.1x NAC) Statistics

Syntax: **show dot1x statistics** { eapol | radius | all } [interface (<port_type> [<v_port_type_list>])]

Description: Display the current IEEE 802.1x NAC statistics. Shows statistics for either *EAPOL* or *RADIUS*, where:
EAPOL (Extensible Authentication Protocol over LAN) is an authentication framework frequently used in wireless networks and point-to-point connections. It is defined in RFC 3748, which made RFC 2284 obsolete, and was updated by RFC 5247.
RADIUS (Remote Authentication Dial In User Service) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service.

Mode: #

Example 1: Show all IEEE 802.1x statistics:

```
# show dot1x statistics all
GigabitEthernet 1/1 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

GigabitEthernet 1/1 Backend Server Statistics:

Rx Access Challenges:                   0   Tx Responses:
    0
Rx Other Requests:                      0
Rx Auth. Successes:                     0
Rx Auth. Failures:                      0

GigabitEthernet 1/2 EAPOL Statistics:
-- more --, next page: Space, continue: g, quit: ^C
```

Example 2: Show IEEE 802.1x statistics sub-sets:

```
# show dot1x statistics eapol ?
    |            Output modifiers
    interface    Interface
    <cr>
# show dot1x statistics eapol
                      Rx      Tx      Rx      Tx      Rx      Tx      Rx      Rx      Rx
Interface             Total   Total   RespId  ReqId   Resp    Req     Start   Logoff  Error
--------------------  ------  ------  ------  ------  ------  ------  ------  ------  -----
GigabitEthernet 1/1   0       0       0       0       0       0       0       0       0
GigabitEthernet 1/2   0       0       0       0       0       0       0       0       0
GigabitEthernet 1/3   0       0       0       0       0       0       0       0       0
GigabitEthernet 1/4   0       0       0       0       0       0       0       0       0
10GigabitEthernet 1/1 0       0       0       0       0       0       0       0       0
       0
       0
# show dot1x statistics eapol interface ?
    *                    All switches or All ports
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
```

Command: Show IEEE 802.1x NAC Status

Syntax: **show dot1x status** [interface (<port_type> [<v_port_type_list>])] [brief]
Description: Display the current IEEE 802.1x NAC status.
Mode: #
Example 1: Show IEEE 802.1x status, such as admin state, port state and last source.

```
# show dot1x status ?
    |            Output modifiers
    brief        Show status in a brief format
    interface    Interface
    <cr>
# show dot1x status | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show dot1x status | begin ?
    LINE    String to match output lines
# show dot1x status interface ?
    *                    All switches or All ports
    ManagementPort       Management Port
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
# show dot1x status
GigabitEthernet 1/1 :
---------------------
Admin State         Port State               Last Source        Last ID
------------------  ---------------------    -----------------  -------------
Force Authorized    Globally Disabled        -                   -

Current Radius QOS    Current Radius VLAN   Current Guest VLAN
--------------------  --------------------  ---------------------
-                     -

GigabitEthernet 1/2 :
---------------------
Admin State         Port State             Last Source        Last ID
------------------  ---------------------  -----------------  -------------
Force Authorized    Globally Disabled      -                  -

Current Radius QOS    Current Radius VLAN   Current Guest VLAN
--------------------  --------------------  ---------------------
-                     -

GigabitEthernet 1/3 :
---------------------
-- more --, next page: Space, continue: g, quit: ^C
# show dot1x status brief
Inf       Admin  Port State  Last Src           Last ID            QOS   VLAN  Guest
--------  -----  ----------  -----------------  -----------------  ----  ----  ------
Mgmt 1/1  Auth   Disabled    -                  -                  -     -     -
Gi 1/1    Auth   Disabled    -                  -                  -     -     -
Gi 1/2    Auth   Disabled    -                  -                  -     -     -
Gi 1/3    Auth   Disabled    -                  -                  -     -     -
Gi 1/4    Auth   Disabled    -                  -                  -     -     -
Gi 1/5    Auth   Disabled    -                  -                  -     -     -
Gi 1/6    Auth   Disabled    -                  -                  -     -     -
Gi 1/7    Auth   Disabled    -                  -                  -     -     -
Gi 1/8    Auth   Disabled    -                  -                  -     -     -
-- more --, next page: Space, continue: g, quit: ^C
```

Command: Show EPS (Ethernet Protection Switching) Config

Syntax: **show eps** [<inst>] [detail]
Description: Display the current EPS configuration.
| Output modifiers:
begin Begin with the line that matches.
exclude Exclude lines that match.
include Include lines that match.
<**Inst** : range_list> The range of EPS instances.
detail Show detailed state including configuration information.
<**cr**>
Mode:
Example 1: Show the **eps** command options.

```
# show eps ?
    |               Output modifiers
    <range_list>    The range of EPS instances.
    detail          Show detailed state including configuration information.
    <cr>
# show eps?
    eps     Ethernet Protection Switching
    <cr>
# show eps??
show eps [ <inst> ] [ detail ]
# show eps

EPS state is:
    Inst       State     Wstate     Pstate     TxAps r b     RxAps r b     FopPm     FopCm     FopNr
FopNoAps

#
```

Example 2: Show the EPS details. The EPS configuration shown is:

```
# show eps detail
EPS state is:
Inst State Wstate Pstate TxAps r b RxAps r b FopPm FopCm FopNr FopNoAps
1 NoReqW Ok Ok NR 0 0 NR 0 0 False False False False
```

EPS Parameters

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.

Command: Show ERPS (Ethernet Ring Protection Switching) Config

Syntax: **show erps** [<groups>] [detail | statistics]

Description: Display the current Ethernet Ring Protection Switching (ERPS) configuration.

1~64 : Zero or more ERPS group numbers.
| : Output modifiers.
detail : Show detailed ERPS information.
statistics : Show ERPS statistics.
<cr>

Mode: #

Example 1: Display the various **show erps** command functions.

```
# show erps 1
(L=Link Up/Down; B=Blocked/Unblocked)      Maj RPL  RPL   RPL  FSM   R-APS
Gr Typ V Rev Port 0     L B Port 1     L B Grp Role Port  Blck State TX RX FOP
--+---+-+---+----------+-+-+----------+-+-+---+----+-----+----+-----+--+--+---
 1 M-I 2 Rev Gi 1/1     U B Gi 1/2     U B -   -    -     -    PEND  N     N
 2 S-I 2 Rev Gi 1/2     U B -          U B 1   -    -     -    NONE  N     N
 3 S-I 2 Rev Gi 1/3     U B -          U B 1   -    -     -    NONE  N     N
# show erps ?
    1~64          Zero or more ERPS group numbers
    |             Output modifiers
    detail        Show detailed information
    statistics    Show statistics
    <cr>
# show erps?
    erps    Ethernet Ring Protection Switching
    <cr>
# show erps detail
% No ERPS groups configured.
# show erps statistics
% No ERPS groups configured.
# con ter
(config)# erps 1 major?
    major    Major ring
(config)# erps 1 major ?
    port0    ERPS Port 0 interface
(config)# erps 1 major port0 ?
    interface    Ethernet interface
(config)# erps 1 major port0 interface ?
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
(config)# erps 1 major port0 interface 10GigabitEthernet ?
    PORT_ID    Port ID in 1/1-2
(config)# erps 1 major port0 interface 10GigabitEthernet 1/2 ?
    port1    ERPS Port 1 interface
(config)# erps 1 major port0 interface 10GigabitEthernet 1/2 port1 ?
    interface    Ethernet interface
(config)# $major port0 interface 10GigabitEthernet 1/2 port1 interface ?
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
(config)# $rface 10GigabitEthernet 1/2 port1 interface GigabitEthernet ?
    PORT_ID    Port ID in 1/1-4
(config)# $rface 10GigabitEthernet 1/2 port1 interface GigabitEthernet 1/3 ?
    interconnect    Major ring is interconnected
    <cr>
(config)# $rface 10GigabitEthernet 1/2 port1 interface GigabitEthernet 1/3
(config)# end
```

```
# show erps 1
(L=Link Up/Down; B=Blocked/Unblocked)      Maj RPL  RPL   RPL  FSM   R-APS
Gr Typ V Rev Port 0     L B Port 1     L B Grp Role Port  Blck State TX RX FOP
--+---+-+---+----------+-+-+----------+-+-+---+----+-----+----+-----+--+--+---
 1 Maj 2 Rev 2.5G 1/2   U B Gi 1/3     U B -   -    -     -    NONE  N     N
```

Example 2: Display **erps 1** details.

```
# show erps 1 detail
Grp#  Port 0         Port 1         RPL:Role   Port    Blocking
   1  Gi 1/1         Gi 1/2         -          -       -
    Protected VLANS:
      None
    Protection Group State             :Active
    Port 0 SF MEP                      :3
    Port 1 SF MEP                      :3
    Port 0 APS MEP                     :2
    Port 1 APS MEP                     :3
    WTR Timeout                        :1
    WTB Timeout                        :5500
    Hold-Off Timeout                   :0
    Guard Timeout                      :500
    Node Type                          :Major
    Reversion                          :Revertive
    Version                            :2
    ERPSv2 Administrative 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                :UNBLOCKED
    R-APS Transmission                 :NR BPR 0
    R-APS Port 0 Reception             :NONE
    R-APS Port 1 Reception             :NONE
    FOP Alarm                          :OFF
#
```

Messages: *% No ERPS groups configured.*
% No such ERPS group: 1

ERPS Parameters

Configurable Parameter	Valid Range	Default
ERPS Id	1-64	1
Port 0 (East port)	Valid port range	1
Port 1 (West Port)	Valid port range	1
	Port 0 SF MEP 1-32	1
	Port 1 SF MEP 1-32	1
	Port 0 APS MEP 1-32	1
	Port 1 APS MEP 1-32	1
	Ring type Major/Sub	Major
Interconnected Node	Yes/No	No
Virtual Channel	Yes/No	No
Major Ring Id (Interconnected Sub ring)	0-99	0

Configurable Parameter	Valid Range	Default
Instance Configuration		
Guard Time	10ms-2000ms, in steps of 10 ms	500 ms
WTR Time	1min, 5min - 12min	1 min
WTB (Hold Off Time)	0ms - 10000ms, in steps of 100ms	0 ms
Version	v1/v2	v2
Revertive	Enable/Disable	Enable
VLAN Config		
VLAN ID	1-4094	N/A
RPL Configuration		
Role	None / RPL_Owner / RPL_Neighbour	None
Port	Port0 / Port1	None
Instance Command		
Command	None, Manual Switch, Forced Switch	None
Port	Port0 / Port1	None

Command: Show EtherSAT

Syntax: **show ethersat config**
show ethersat loopback { config | state | testsideport | smac | vid | timeout }
show ethersat loopback { status }
show ethersat profile <pid> config
show ethersat profile <pid> frameformat

Description: Display the current Ethernet Service Activation Test (SAT) configuration and statistics. Note that the Shared Port must be set to Internal mode.

Mode: #

Example 1: Display the various **show ethersat** command functions.

```
# show ethersat ?
    config      Show ethersat configuration status.
    loopback    TN ethersat loopback
    profile
# show ethersat??
    ethersat    ethersat (Service Activation Test)
# show ethersat?
show ethersat config
show ethersat loopback { config | state | testsideport | smac | vid | timeout }

show ethersat loopback { status }
show ethersat profile <pid> config
show ethersat profile <pid> frameformat
# show ethersat config

EtherSAT Configuration:
=======================

Collector:            enabled
Peer channel:         enabled
Test MAC Address:     00:c0:f2:56:16:e8
# show ethersat loopback ?
    config          Show the ethersat loopback configuration status.
    smac            Show the ethersat loopback SMAC address.
    state           Show the ethersat loopback state.
    status          Show ethersat loopback Status
    testsideport    Show the ethersat loopback TestSidePort port number.
    timeout         Show the ethersat loopback timeout.
    vid             Show the ethersat loopback Vlan ID.
# show ethersat loopback config

ethersat loopback Configuration:
================================

State    testSidePort SMAC              vid Timeout
-------- ------------ ----------------- --- -------
Inactive 1            00:00:00:00:00:01 1    300

# show ethersat loopback smac
ethersat loopback SMAC: 00:00:00:00:00:01
# show ethersat loopback state
ethersat loopback State: Inactive
# show ethersat loopback status

ethersat loopback Status:
=========================

State: Inactive
```

```
Frames: 0, Bytes: 0
# show ethersat loopback testsideport
ethersat loopback TestSidePort: 1
# show ethersat loopback timeout
ethersat loopback Timeout: 300
# show ethersat profile 1 ?
    config         Show ethersat profile config status.
    frameformat    Show ethersat profile frame format status.
# show ethersat profile 1 config ?
    |       Output modifiers
    <cr>
# show ethersat profile 1 config
Profile ID:               1
Name:                     SatTest1
Frame Loss Ratio:         0.00 %
Coloring method:          PCP
Yellow Frames PCP Values: 0 1
Frame Size Mix:           64
Rate Decrease Step:       25 %
Step Length:              10 sec
Exit on Fail:             enabled
Test Mode:                unidir
Test Steps:               throughput latency flr back-to-back
Reference Number:         0
CBS line rate:            1000 Mbps
DM Thresholds, us:
                          [      0 - 5000000]
                          [        > 5000000]
DMV Thresholds, us:
                          [      0 - 5000000]
                          [        > 5000000]
# show ethersat profile ?
    <1-16>    Profile ID.
# show ethersat profile 1 ?
    config         Show ethersat profile config status.
    frameformat    Show ethersat profile frame format status.
# show ethersat profile 1 frameformat
Level:                    L2
Encapsulation Type:       ETH-TST
Filling Mode:             PRBS
Frame Payload Pattern:    0x00000000
Custom EthType:           0x8902
LLC/SNAP OUI:             00-00-00
LLC/SNAP Protocol:        0x0000
SOAM MEG Level:           5
IP Header:
  Destination IP Address: 0.0.0.0
  Source IP Address:      0.0.0.0
  DSCP:                   0
  ECN:                    0
  Flags:                  0
  TTL:                    0
UDP Header:
  Source Port:            0
  Destination Port:       0
TCP Header:
  Source Port:            0
  Destination Port:       0
  Sequence Number:        0
-- more --, next page: Space, continue: g, quit: ^C
```

Command: Show EVC Info

Syntax: **show evc statistics** { [<evc_id> | all] } [ece [<ece_id>]] [interface (<port_type> [<port_list>])] [pw <pw_num_list>] [cos <cos>] [green | yellow | red | discard] [frames | bytes]
show evc { [<evc_id> | all] } [ece [<ece_id>]]

Description: Display the current Ethernet Virtual Connection (EVC) configuration and statistics.

Mode: #

Example 1:

```
# show evc ?
    |             Output modifiers
    <1-4096>      EVC identifier
    all           Process all EVCs
    ece           EVC Control Entry
    statistics    Statistic counters
    <cr>
# show evc
EVC ID  Status
------  ------
1       Active

#
# show evc ?
    |             Output modifiers
    <1-256>       EVC identifier
    all           Process all EVCs
    ece           EVC Control Entry
    statistics    Statistic counters
    <cr>
# show evc all
EVC ID  Status
------  ------
1       Active
# show evc <cr>
EVC ID  Status
------  ------
1       Active

ECE ID  Status
------  ------
1       Active
2       Active
#
```

Example 2:

```
# show evc ece?
    ece     EVC Control Entry
    <cr>
# show evc ece ?
    |                 Output modifiers
    <EceId : 1-256>   ECE idenfifier
    <cr>
# show evc 1 ece ?
    |                 Output modifiers
    <EceId : 1-256>   ECE idenfifier
    <cr>
# show evc 1 ece 1
# show evc ece | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show evc ece
```

```
ECE ID  Status
------  ------
1       Active
2       Active
#
```

Example 3:

```
# show evc statistics ?
    |            Output modifiers
    <1-4096>      EVC identifier
    all          Process all EVCs
    bytes        Byte counters
    discard      Discard counters
    ece          EVC Control Entry
    frames       Frame counters
    green        Green counters
    interface    Interface
    pw           Show EVC statistics for attached MPLS-TP Pseudo-Wires
    red          Red counters
    yellow       Yellow counters
    <cr>
```

Example 4: Display EVC statistics for an interface.

```
# show evc statistics
EVC ID 1, Interface GigabitEthernet 1/2 Statistics:

Rx Green Frames:                     0   Tx Green Frames:                0
Rx Yellow Frames:                    0   Tx Yellow Frames:               0
Rx Red Frames:                       0
Rx Discard Frames:                   0   Tx Discard Frames:              0
Rx Green Bytes:                      0   Tx Green Bytes:                 0
Rx Yellow Bytes:                     0   Tx Yellow Bytes:                0
Rx Red Bytes:                        0
Rx Discard Bytes:                    0   Tx Discard Bytes:               0

EVC ID 1, Interface GigabitEthernet 1/3 Statistics:

Rx Green Frames:                     0   Tx Green Frames:                0
Rx Yellow Frames:                    0   Tx Yellow Frames:               0
Rx Red Frames:                       0
Rx Discard Frames:                   0   Tx Discard Frames:              0
Rx Green Bytes:                      0   Tx Green Bytes:                 0
Rx Yellow Bytes:                     0   Tx Yellow Bytes:                0
Rx Red Bytes:                        0
Rx Discard Bytes:                    0   Tx Discard Bytes:               0

-- more --, next page: Space, continue: g, quit: ^C
```

Note: If EVC ID1 is configured for an ECE via the webGUI or CLI, the CLI does not display EVC1. If any EVC ID>1 is configured, it is displayed.

Command: Show Green Ethernet (Power Reduction)

Syntax: **show green-ethernet** [interface (<port_type> [<port_list>])]
show green-ethernet energy-detect [interface (<port_type> [<port_list>])]
show green-ethernet short-reach [interface (<port_type> [<port_list>])]

Description: Display the current Green Ethernet (Power reduction) configurations.

Mode: #

Example: Display the command variations:

```
# show green-ethernet ?
    |                 Output modifiers
    energy-detect     Shows green ethernet energy-detect status for a specific
                      port or ports.
    interface         Shows green ethernet status for a specific port or ports.
    short-reach       Shows green ethernet short-reach status for a specific
                      port or ports.
    <cr>
# show green-ethernet?
    green-ethernet    Green ethernet (Power reduction)
    <cr>
# show green-ethernet?
show green-ethernet [ interface <port_type_list> ]
show green-ethernet energy-detect [ interface <port_type_list> ]
show green-ethernet short-reach [ interface <port_type_list> ]
# show green-ethernet energy-detect interface ?
    *                    All switches or All ports
    ManagementPort       Management Port
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
# show green-ethernet
# show green-ethernet
Interface               Energy-detect  Short-Reach
----------------------  -------------  ------------
ManagementPort 1/1      No             No
GigabitEthernet 1/1     N/A            N/A
GigabitEthernet 1/2     N/A            N/A
GigabitEthernet 1/3     N/A            N/A
GigabitEthernet 1/4     N/A            N/A
GigabitEthernet 1/5     N/A            N/A
GigabitEthernet 1/6     N/A            N/A
GigabitEthernet 1/7     N/A            N/A
GigabitEthernet 1/8     N/A            N/A
GigabitEthernet 1/9     N/A            N/A
GigabitEthernet 1/10    N/A            N/A
-- more --, next page: Space, continue: g, quit: ^C
```

Energy Detect Mode: moves a port into inactive mode if the link is inactive. This saves power while keeping the administrative status of the port up.

Short Reach: Traditional Ethernet transmits all data with enough power to reach the maximum cable length. Shorter cables lose less power, so Short Reach saves power by adjusting the transmit power of each port according to the length of cable attached to that port.

Command: Show History of CLI Session

Syntax: **show history**
Description: Display the latest session command history since the last login.
Mode: #

Example 1:

```
# show history ?
    |       Output modifiers
    <cr>
# show history | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show history |
```

Example 2:

```
# show history ?
    |       Output modifiers
    <cr>
# show history
  show clock
  show clock detail
  show ddmi
  show dot1x statistics
  show dot1x statistics all
  show dot1x statistics eapol
  show dot1x status
  show dot1x status brief
  show eps
  show erps
  con ter
  end
  show erps detail
  show erps 1 detail
  show erps 1 statistics
  show ethersat config
  show ethersat loopback config
  show ethersat loopback smac
  show ethersat loopback state
  show ethersat loopback status
  show ethersat loopback testsideport
  show ethersat loopback timeout
-- more --, next page: Space, continue: g, quit: ^C
```

Command: Show Interface Status and Configuration

Syntax: **show interface** (<port_type> [<in_port_list>]) **switchport** [access | trunk |hybrid]
show interface (<port_type> [<plist>]) **transceiver**
show interface (<port_type> [<v_port_type_list>]) **capabilities**
show interface (<port_type> [<v_port_type_list>]) **statistics** [{ packets | bytes | errors | discards | filtered | { priority [<priority_v_0_to_7>] } }] [{ up | down }]
show interface (<port_type> [<v_port_type_list>]) **status**
show interface (<port_type> [<v_port_type_list>]) **veriphy**
show interface tunnel-tp [<tunnel_tp_num>] [statistics]
show interface vlan [<vlist>]

Description: Display the current Interface status and configuration.

Mode: #

Example 1: Show interface command options:

```
# show interface ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
    vlan                VLAN status
# show interface?
    interface    Interface status and configuration
# show interface??
show interface ( <port_type> [ <in_port_list> ] ) switchport [ access | trunk |hybrid ]
show interface ( <port_type> [ <plist> ] ) transceiver
show interface ( <port_type> [ <v_port_type_list> ] ) capabilities
show interface ( <port_type> [ <v_port_type_list> ] ) statistics [ { packets | bytes | errors
| discards | filtered | { priority [ <priority_v_0_to_7> ] } } ] [ { up | down } ]
show interface ( <port_type> [ <v_port_type_list> ] ) status
show interface ( <port_type> [ <v_port_type_list> ] ) veriphy
show interface vlan [ <vlist> ]
# show interface?
    interface    Interface status and configuration
# show interface
```

Example 2: Show 1 Gigabit Ethernet Port options:

```
# show interface g 1/1 ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
    capabilities        Display capabilities.
    statistics          Display statistics counters.
    status              Display status.
    switchport          Show interface switchport information
    transceiver         Show interface transceiver
    veriphy             Run cable diagnostics and show result.
# show interface g 1/1
```

Example 3: Show interface status, switchport, and VeriPHY:

```
# show interface g 1/1 status
Interface               Mode     Speed & Duplex  Flow Control  Max Frame  Excessive  Link
----------------------  -------  --------------  ------------  ---------  ---------  --------
GigabitEthernet 1/1     enabled  Auto            disabled      4776       Discard    1Gfdx Fbr
# show interface g 1/1 switchport ?
    |         Output modifiers
    access    Show access ports status
    hybrid    Show hybrid ports status
    trunk     Show trunk ports status
    <cr>
# show interface g 1/1 switchport
Name: GigabitEthernet 1/1
Administrative mode: access
Access Mode VLAN: 1
Trunk Native Mode VLAN: 1
Administrative Native VLAN tagging: disabled
Allowed VLANs: 1-4094
Hybrid port configuration
-------------------------
Port Type: C-Port
Acceptable Frame Type: All
Ingress filter: Disabled
Egress tagging: All except-native
Hybrid Native Mode VLAN: 1
Hybrid VLANs Enabled: 1-4094

#

# show interface g 1/1 veriphy
Starting VeriPHY - Please wait
Interface               Pair A  Length  Pair B, Length  Pair C  Length  Pair D Length
----------------------  ------  ------  --------------  ------  ------  -------------
GigabitEthernet 1/1     Open    0       Open    0       Open    0       Open    0
```

Example 4: Show interface switchport access and trunk:

```
# show interface g 1/1 switchport hybrid
Name: GigabitEthernet 1/1
Administrative mode: hybrid
Access Mode VLAN: 1
Trunk Native Mode VLAN: 1
Administrative Native VLAN tagging: disabled
VLAN Trunking: disabled
Allowed VLANs: 1-4095
Hybrid port configuration
-------------------------
Port Type: Unaware
Acceptable Frame Type: All
Ingress filter: Disabled
Egress tagging: All except-native
Hybrid Native Mode VLAN: 1
Hybrid VLANs Enabled: 1
# show interface g 1/1 switchport trunk?
```

```
    trunk    Show trunk ports status
    <cr>
# show interface g 1/1 switchport trunk ?
    |       Output modifiers
    <cr>
```

Example 5: Show interface capabilities and statistics:

```
# show interface * ?
    <port_type_list>    Port list for all port types
    capabilities        Display capabilities.
    statistics          Display statistics counters.
    status              Display status.
    switchport          Show interface switchport information
    transceiver         Show interface transceiver
    veriphy             Run cable diagnostics and show result.
# show interface * 1/1 ?
    *                    All switches or All ports
    ManagementPort       Management Port
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
    capabilities         Display capabilities.
    statistics           Display statistics counters.
    status               Display status.
    switchport           Show interface switchport information
    transceiver          Show interface transceiver
    veriphy              Run cable diagnostics and show result.
# show interface *  1/1 capabilities

GigabitEthernet 1/1 Capabilities:
  Name/Model:            Transition      TN-SFP-SXD
  Type:                  1000BASE_SX
  Speed:                 1000,auto
  Duplex:                full,auto
  Trunk encap. type:     802.1Q
  Trunk mode:            access,hybrid,trunk
  Channel:               yes
  Broadcast suppression: no
  Flowcontrol:           no
  Fast Start:            no
  QoS scheduling:        tx-(8q)
  CoS rewrite:           yes
  ToS rewrite:           yes
  UDLD:                  no
  Inline power:          no
  RMirror:               yes
  PortSecure:            yes
  Dot1x:                 yes

10GigabitEthernet 1/1 Capabilities:
-- more --, next page: Space, continue: g, quit: ^C
```

Example 6: Show interface statius and switchport info:

```
# show interface * 1/1 status
Interface               Mode     Speed & Duplex  Flow Control  Max Frame  Excessive  Link
----------------------  -------  --------------  ------------  ---------  ---------  --------
GigabitEthernet 1/1     enabled  Auto            disabled      4776       Discard    1Gfdx Fbr
10GigabitEthernet 1/1   enabled  10Gfdx          disabled      4776       Discard    Down
# show interface * 1/1 switchport ?
    |         Output modifiers
    access    Show access ports status
    hybrid    Show hybrid ports status
    trunk     Show trunk ports status
    <cr>
# show interface * 1/1 switchport
Name: GigabitEthernet 1/1
Administrative mode: access
Access Mode VLAN: 1
Trunk Native Mode VLAN: 1
Administrative Native VLAN tagging: disabled
Allowed VLANs: 1-4094
Hybrid port configuration
-------------------------
Port Type: C-Port
Acceptable Frame Type: All
Ingress filter: Disabled
Egress tagging: All except-native
Hybrid Native Mode VLAN: 1
Hybrid VLANs Enabled: 1-4094

Name: 10GigabitEthernet 1/1
Administrative mode: access
Access Mode VLAN: 1
Trunk Native Mode VLAN: 1
Administrative Native VLAN tagging: disabled
Allowed VLANs: 1-4094
Hybrid port configuration
-- more --, next page: Space, continue: g, quit: ^C
```

Example 7: Show Interface Port VeriPhy:

```
# show interface GigabitEthernet 1/1 veriphy
Starting VeriPHY - Please wait
Interface               Pair A  Length  Pair B, Length  Pair C  Length  Pair D Length
----------------------  ------  ------  --------------  ------  ------  -------------
GigabitEthernet 1/1     OK      0       OK      0       Short   0       Open   3
GigabitEthernet 1/2     No test results
GigabitEthernet 1/3     No test results
GigabitEthernet 1/4     No test results
GigabitEthernet 1/5     No test results
10GigabitEthernet 1/1  No test results
10GigabitEthernet 1/2  No test results
# show interface * veriphy
Interface               Pair A  Length  Pair B, Length  Pair C  Length  Pair D  Length
----------------------  ------  ------  --------------  ------  ------  ------  -------
ManagementPort 1/1      No test results
GigabitEthernet 1/1     No test results
GigabitEthernet 1/2     No test results
GigabitEthernet 1/3     No test results
GigabitEthernet 1/4     No test results
GigabitEthernet 1/5     No test results
GigabitEthernet 1/6     No test results
GigabitEthernet 1/7     No test results
GigabitEthernet 1/8     No test results
GigabitEthernet 1/9     No test results
GigabitEthernet 1/10    No test results
GigabitEthernet 1/11    No test results
GigabitEthernet 1/12    No test results
GigabitEthernet 1/13    No test results
GigabitEthernet 1/14    No test results
GigabitEthernet 1/15    No test results
GigabitEthernet 1/16    No test results
GigabitEthernet 1/17    No test results
#
```

The VeriPHY diagnostic takes approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters. The 10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete. The VeriPhy parameters are:

Pair: The status of the cable pair. The displayable values are:
OK - Correctly terminated pair
Open - Open pair.
Short - Shorted pair.
Short A-D - Cross-pair short to pair A thru D.
Cross A-D - Abnormal cross-pair coupling with pair A thru D.

Length: The length (in meters) of the cable pair. The resolution is 3 meters.

Example 7: Show Interface VLAN:

```
# show interface vlan
VLAN1
  LINK: 00-c0-f2-56-1a-90 Mtu:1500 <UP BROADCAST RUNNING MULTICAST>
  IPv4: 192.168.1.110/24 192.168.1.255
  IPv6: fe80::2c0:f2ff:fe56:1a90/64 <ANYCAST TENTATIVE AUTOCONF>
# show interface vlan 1
VLAN1
  LINK: 00-c0-f2-56-1a-90 Mtu:1500 <UP BROADCAST RUNNING MULTICAST>
  IPv6: fe80::2c0:f2ff:fe56:1a90/64 <ANYCAST TENTATIVE AUTOCONF>
  IPv4: 192.168.1.110/24 192.168.1.255
# show interface vlan 10
% VLAN interface 10 does not exist.
#
```

Example 8: Show InterfaceTransceiver (DDMI) information:

```
# show interface G 1/1-12 transceiver

GigabitEthernet 1/1
------------------------------
Tranceiver Information
================================================================================
Vendor             : Transition
Part Number        : TN-SFP-SXD
Serial Number      : 8672105
Revision           : 0000
Date Code          : 2009-10-27
Transceiver        : 1000BASE_SX

DDMI Information
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.
================================================================================
              current   High Alarm   High Warn    Low Warn      Low Alarm
                         Threshold    Threshold    Threshold     Threshold
-------------  --------  ----------   ----------   ----------    --------
Temperature(C) 37.000      95.000       85.000       -5.000       -10.000
Voltage(V)     3.2864      3.6000       3.5000       3.1000       3.0000
Tx Bias(mA)    14.480      20.000       15.000       2.000        1.000
-- more --, next page: Space, continue: g, quit: ^C
```

Command: Show Internet Protocol (IP) Configs

Syntax: **show ip**

Description: Display the current IP configurations for ARP, DHCP, Domain, HTTP, IGMP, IP IF, DNS, IP routing, Traffic stats, and verify command.

Mode: #

Example 1: Show the various IP command paraeters:

```
# show ip ?
    arp             Address Resolution Protocol
    dhcp            Dynamic Host Configuration Protocol
    domain          Default domain name
    http            Hypertext Transfer Protocol
    igmp            Internet Group Management Protocol
    interface       IP interface status and configuration
    name-server     Domain Name System
    route           Display the current ip routing table
    source          source command
    ssh             Secure Shell
    statistics      Traffic statistics
    verify          verify command
```

Example 2: Show the various IP ARP command parameters:

```
# show ip arp
192.168.1.30 via VLAN1:00-04-75-bd-9c-36
# show ip arp ?
    |              Output modifiers
    inspection     ARP inspection
    <cr>
# show ip arp inspection ?
    |             Output modifiers
    entry         arp inspection entries
    interface     arp inspection entry interface config
    vlan          VLAN configuration
    <cr>
# show ip arp inspection
ARP Inspection Mode : disabled

Port                      Port Mode   Check VLAN  Log Type
----                      ---------   ----------  --------
ManagementPort 1/1        disabled    disabled    NONE
GigabitEthernet 1/1       disabled    disabled    NONE
GigabitEthernet 1/2       disabled    disabled    NONE
GigabitEthernet 1/3       disabled    disabled    NONE
GigabitEthernet 1/4       disabled    disabled    NONE
GigabitEthernet 1/5       disabled    disabled    NONE
GigabitEthernet 1/6       disabled    disabled    NONE
GigabitEthernet 1/7       disabled    disabled    NONE
GigabitEthernet 1/8       disabled    disabled    NONE
GigabitEthernet 1/9       disabled    disabled    NONE
GigabitEthernet 1/10      disabled    disabled    NONE
GigabitEthernet 1/11      disabled    disabled    NONE
GigabitEthernet 1/12      disabled    disabled    NONE
-- more --, next page: Space, continue: g, quit: ^C
```

Example 3: Show the various IP DHCP, HTTP, IGMP, and Interface command parameters:

```
# show ip dhcp ?
    detailed            DHCP server statistics
    excluded-address    Excluded IP database
    forwarding     Forwarding of DHCP traffic to/from this port
    pool                DHCP pools information
    relay               DHCP relay agent configuration/statistics
    server              DHCP server info (status/binding/ declined-ip/ statistics)
    snooping            DHCP snooping info (status/interface/table)

# show ip http ?
    server    HTTP web server
# show ip http server secure status
Switch secure HTTP web server is disabled
Switch secure HTTP web redirection is disabled
Switch secure HTTP certificate is presented
# show ip igmp snooping ?
    |                 Output modifiers
    detail            Detail running information/statistics of IGMP snooping
    group-database    Multicast group database from IGMP
    mrouter           Multicast router port status in IGMP
    vlan              Search by VLAN
    <cr>
# show ip interface brief
Vlan Address              Method   Status
---- -------------------- -------- ------
   1 192.168.1.110/24     Manual   DOWN
# show ip name-server | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show ip route | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show ip route
127.0.0.1/32 via 127.0.0.1 <UP HOST>
192.168.1.0/24 via interface index 1 <UP HW_RT>
224.0.0.0/4 via 127.0.0.1 <UP>
#
# show ip source binding ?
    dhcp-snooping    learn from dhcp snooping
    interface        ip source binding interface config
    static           setting from static entries
    <cr>
# show ip statistics ?
    |            Output modifiers
    icmp         IPv4 ICMP traffic
    icmp-msg     IPv4 ICMP traffic for designated message type
    interface    Select an interface to configure
    system       IPv4 system traffic
    <cr>
# show ip verify source ?
    interface    ip verify source interface config
    <cr>
# show ip verify source interface ?
    *                    All switches or All ports
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    2.5 Gigabit Ethernet Port
# show ip verify source interface *
```

```
Port                      Port Mode    Dynamic Entry Limit
----                      ---------    -------------------
GigabitEthernet 1/1       disabled     unlimited
GigabitEthernet 1/2       disabled     unlimited
GigabitEthernet 1/3       disabled     unlimited
GigabitEthernet 1/4       disabled     unlimited
GigabitEthernet 1/5       disabled     unlimited
GigabitEthernet 1/6       disabled     unlimited

Port                      Port Mode    Dynamic Entry Limit
----                      ---------    -------------------
GigabitEthernet 1/7       disabled     unlimited
GigabitEthernet 1/8       disabled     unlimited

Port                      Port Mode    Dynamic Entry Limit
----                      ---------    -------------------
10GigabitEthernet 1/1     disabled     unlimited
10GigabitEthernet 1/2     disabled     unlimited
#
```

Show IP Command / Parameters Summary

show ip arp
show ip arp inspection [interface (<port_type> [<in_port_type_list>]) | vlan <in_vlan_list>]
show ip arp inspection entry [dhcp-snooping | static] [interface (<port_type> [<in_port_type_list>])]
show ip dhcp detailed statistics { server | client | snooping | relay | normal-forward | combined } [interface (<port_type> [<in_port_list>])]
show ip dhcp excluded-address
show ip dhcp pool [<pool_name>]
show ip dhcp relay [statistics]
show ip dhcp server
show ip dhcp server binding <ip>
show ip dhcp server binding [state { allocated | committed | expired }] [type { automatic | manual | expired }]
show ip dhcp server declined-ip
show ip dhcp server declined-ip <declined_ip>
show ip dhcp server statistics
show ip dhcp snooping [interface (<port_type> [<in_port_list>])]
show ip dhcp snooping table
show ip domain
show ip http server secure status
show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show ip igmp snooping mrouter [detail]
show ip interface brief
show ip name-server
show ip route
show ip source binding [dhcp-snooping | static] [interface (<port_type> [<in_port_type_list>])]
show ip ssh
show ip statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]
show ip verify source [interface (<port_type> [<in_port_type_list>])]

Command: Show IPv4/IPv6 Multicast Configuration

Syntax: **show ipmc profile** [<profile_name>] [detail]
show ipmc range [<entry_name>]
Description: Display the current IPv4/IPv6 multicast configuration parameters.
Mode: #
Example: Display the various command options.

```
# show ipmc ?
    profile    IPMC profile configuration
    range      A range of IPv4/IPv6 multicast addresses for the profile
# show ipmc profile ?
    |                          Output modifiers
    <ProfileName : word16>     Profile name in 16 char's
    detail                     Detail information of a profile
    <cr>
# show ipmc profile

IPMC Profile is now enabled to start filtering.

Profile: Tst1 (In VER-INI Mode)
Description: IPMCProf1

Profile: Tst2 (In VER-INI Mode)
Description: IPMCProf2
# show ipmc profile detail

IPMC Profile is now enabled to start filtering.

Profile: Tst1 (In VER-INI Mode)
Description: IPMCProf1

IGMP will deny matched address between [224.0.0.0 <-> 239.255.255.255]
MLD will deny matched address between [ff00:: <-> ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff]

Profile: Tst2 (In VER-INI Mode)
Description: IPMCProf2

IGMP will deny matched address between [224.0.0.0 <-> 239.255.255.255]
MLD will deny matched address between [ff00:: <-> ffff:ffff:ffff:ffff:ffff:ffff:
ffff:ffff]
# show ipmc range

Range Name   : one
Start Address: 224.0.0.1
End Address  : 224.0.0.100
#
# show ipmc profile range detail

IPMC Profile is currently disabled, please enable profile to start filtering.

Profile: range (In VER-INI Mode)
Description:

IGMP will deny matched address between [224.0.0.0 <-> 239.255.255.255]
MLD will deny matched address between [ff00:: <-> ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff]
#
```

Messages: *% Invalid profile name a.*
IPMC Profile is currently disabled, please enable profile to start filtering.

Command: Show IPv6 Config

Syntax: **show ipv6 dhcp-client** [interface vlan <v_vlan_list>]
show ipv6 interface [vlan <v_vlan_list> { brief | statistics }]
show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
show ipv6 mld snooping mrouter [detail]
show ipv6 neighbor [interface vlan <v_vlan_list>]
show ipv6 route [interface vlan <v_vlan_list>]
show ipv6 statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

Description: Display the current IPv6 configuration commands for:
dhcp client Manage DHCPv6 client service
interface Select an interface to configure
mld Multicasat Listener Discovery
neighbor IPv6 neighbors
route IPv6 routes
statistics Traffic statistics

Mode: #

Example 1: show ipv6 dhcp-client:

```
# show ipv6 dhcp-client?
    dhcp-client    Manage DHCPv6 client service
    <cr>
# show ipv6 dhcp-client?
show ipv6 dhcp-client [ interface vlan <v_vlan_list> ]
# show ipv6 dhcp-client?
    dhcp-client    Manage DHCPv6 client service
    <cr>
# show ipv6 dhcp-client
#
```

Example 2: show ipv6 interface vlan 1 brief and detail:

```
# show ipv6 interface vlan 1 brief

IPv6 Vlan1 interface is down.
  Internet address is fe80::2c0:f2ff:fe21:db83
  Static address is not set
# show ipv6 mld snooping detail vlan 1

MLD Snooping is disabled to stop snooping MLD control plane.
Multicast streams destined to unregistered MLD groups will be flooding.
# show ipv6 statistics ?
    |            Output modifiers
    icmp         IPv6 ICMP traffic
    icmp-msg     IPv6 ICMP traffic for designated message type
    interface    Select an interface to configure
    system       IPv6 system traffic
    <cr>
# show ipv6 statistics
```

Example 3: Show IPv6 stats:

```
# show ipv6 statistics icmp ?
    |            Output modifiers
    icmp-msg     IPv6 ICMP traffic for designated message type
    interface    Select an interface to configure
    system       IPv6 system traffic
    <cr>
# show ipv6 statistics icmp icmp-msg ?
    <Type : 0~255>    ICMP message type ranges from 0 to 255
# show ipv6 statistics icmp interface ?
    vlan    IPv6 interface traffic
```

```
# show ipv6 statistics icmp interface vlan ?
    <vlan_list>    VLAN identifier(s): VID
# show ipv6 statistics icmp interface vlan 1

IP interface statistics:

  IPv6 Statistics on Interface VLAN: 1
  Rcvd:  0 total in 0 byte
         0 local destination, 0 forwarding
         0 header error, 0 address error, 0 unknown protocol
         0 no route, 0 truncated, 0 discarded
  Sent:  10 total in 656 bytes
         10 generated, 0 forwarded
         0 discarded
  Frags: 0 reassemble (0 reassembled, 0 couldn't reassemble)
         0 fragment (0 fragmented, 0 couldn't fragment)
         0 fragment created
  Mcast: 0 received in 0 byte
         10 sent in 656 bytes
  Bcast: 0 received, 0 sent

IPv6 ICMP statistics:

  Rcvd: 0 Message, 0 Error
  Sent: 12 Messages, 0 Error
# show ipv6 statistics icmp system ?
    |            Output modifiers
    icmp-msg     IPv6 ICMP traffic for designated message type
    interface    Select an interface to configure
    <cr>
```

Example 4: Show IPv6 stats:

```
# show ipv6 statistics icmp system interface vlan 1

IPv6 statistics:

  Rcvd:  0 total in 0 byte
         0 local destination, 0 forwarding
         0 header error, 0 address error, 0 unknown protocol
         0 no route, 0 truncated, 0 discarded
  Sent:  10 total in 656 bytes
         14 generated, 0 forwarded
         0 no route, 0 discarded
  Frags: 0 reassemble (0 reassembled, 0 couldn't reassemble)
         0 fragment (0 fragmented, 0 couldn't fragment)
         0 fragment created
  Mcast: 0 received in 0 byte
         10 sent in 656 bytes
  Bcast: 0 received, 0 sent

IP interface statistics:

  IPv6 Statistics on Interface VLAN: 1
  Rcvd:  0 total in 0 byte
         0 local destination, 0 forwarding
-- more --, next page: Space, continue: g, quit: ^C
```

Command: Show IP Verify Source Guard Info

Syntax: **show ip verify source** [interface (<port_type> [<in_port_type_list>])]

Description: Display current IP Source Guard mode and ports modes parameters. 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. The parameters are:

IP Source Guard Mode : disabled or enabled. The default is disabled.
Port: e.g., "GigabitEthernet 1/1" or "10GigabitEthernet 1/2".
Port Mode: enabled or disabled.
Dynamic Entry Limit: e.g., unlimited

Mode: #

Example 1:

```
# show ip verify source ?
    interface    ip verify source interface config
    <cr>
# show ip verify source interface ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
# show ip verify source
IP Source Guard Mode : disabled

Port                    Port Mode    Dynamic Entry Limit
----                    ---------    -------------------
ManagementPort 1/1      disabled     unlimited
GigabitEthernet 1/1     disabled     unlimited
GigabitEthernet 1/2     disabled     unlimited
GigabitEthernet 1/3     disabled     unlimited
GigabitEthernet 1/4     disabled     unlimited
GigabitEthernet 1/5     disabled     unlimited
GigabitEthernet 1/6     disabled     unlimited
GigabitEthernet 1/7     disabled     unlimited
GigabitEthernet 1/8     disabled     unlimited
GigabitEthernet 1/9     disabled     unlimited
GigabitEthernet 1/10    disabled     unlimited
GigabitEthernet 1/11    disabled     unlimited
GigabitEthernet 1/12    disabled     unlimited
GigabitEthernet 1/13    disabled     unlimited
GigabitEthernet 1/14    disabled     unlimited
GigabitEthernet 1/15    disabled     unlimited
GigabitEthernet 1/16    disabled     unlimited
GigabitEthernet 1/17    disabled     unlimited
-- more --, next page: Space, continue: g, quit: ^C
```

Command: Show LACP Config / Status

Syntax: **show lacp** { internal | statistics | system-id | neighbour }

Description: Display the current LACP (Link Aggregation Control Protocol) configuration / status. The Link Aggregation Control Protocol, exchanges LACPDUs with an LACP partner and forms an aggregation automatically. LACP can be enabled or disabled on the switch port. LACP will form an aggregation when two or more ports are connected to the same partner. The Key value can be configured to a user defined value or set to Auto to calculate based on the link speed in accordance with IEEE 802.3ad standard. The Role for the LACP Port configuration can be selected as either Active to transmit LACP packets each second or Passive to wait for a LACP packet from a partner.

Mode: #

Example:

```
# show lacp ?
    internal      Internal LACP configuration
    neighbour     Neighbour LACP status
    statistics    Internal LACP statistics
    system-id     LACP system id
# show lacp internal
Port                  Mode      Key   Role    Timeout  Priority
--------------------  --------  ----  ------  -------  --------
Gi 1/1                disabled   Auto  Active  Fast     32768
Gi 1/2                disabled   Auto  Active  Fast     32768
Gi 1/3                disabled   Auto  Active  Fast     32768
Gi 1/4                disabled   Auto  Active  Fast     32768
2.5G 1/1              disabled   Auto  Active  Fast     32768
2.5G 1/2              disabled   Auto  Active  Fast     32768
# show lacp neighbour ?
    |       Output modifiers
    <cr>
# show lacp neighbour

# show lacp statistics ?
    |       Output modifiers
    <cr>
# show lacp statistics
# show lacp system-id
System Priority: 100
# show lacp neighbour | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show lacp statistics | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show lacp system-id ?
    |       Output modifiers
    <cr>
# show lacp system-id
System Priority: 32768
# show lacp system-id | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show lacp system-id |
```

Command: Show TTY Line Information

Syntax: **show line** [alive]
Description: Display the current terminal console line information.
Mode: #
Example:

```
# show line ?
    |        Output modifiers
    alive    Display information about alive lines
    <cr>
# show line
Line is con 0.
    * You are at this line now.
    Alive from Console.
    Default privileged level is 2.
    Command line editing is enabled
    Display EXEC banner is enabled.
    Display Day banner is enabled.
    Terminal width is 80.
             length is 24.
             history size is 32.
             exec-timeout is 10 min 0 second.

    Current session privilege is 15.
    Elapsed time is 0 day 3 hour 18 min 1 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

Line is vty 0.
    Not alive.
    Default privileged level is 2.
    Command line editing is enabled
    Display EXEC banner is enabled.
    Display Day banner is enabled.
    Terminal width is 80.
             length is 24.
             history size is 32.
             exec-timeout is 10 min 0 second.

    Current session privilege is 0.
    Elapsed time is 0 day 0 hour 0 min 0 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

-- more --, next page: Space, continue: g, quit: ^C
```

```
# show line | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show line |
```

Command: Show Link OAM Configuration

Syntax: **show link-oam** { [status] [link-monitor] [statistics] } [interface (<port_type> [<plist>])]

Description: Display the current Link OAM configuration. The OAM capabilities allow an Administrator to install, monitor and troubleshoot the Ethernet MANs and WANs. The S4224 supports OAM functionality in both point-to-point link monitoring as ascribed in IEEE802.3ah and Flow OAM. Flow OAM implementation implements requirements from IEEE802.1ag plus IEEE standards ITU12 T.1731 and ITU-T.G.8021.

Mode: #

Example: Show link OAM config:

```
# show link-oam?
interface     link-monitor  statistics    status        |
<cr>
# show link-oam interface
*                   10GigabitEthernet  GigabitEthernet
# show link-oam statistics

GigabitEthernet 1/1
----------------------------------------
PDU stats
-----------
Information PDU TX:                         0
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
Org Specific PDU RX:                        0
Org Specific PDU TX:                        0
Unsupported PDU RX:                         0
Unsupported PDU TX:                         0
Link Fault PDU TX:                          0
# show link-oam status

GigabitEthernet 1/1
----------------------------------------
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                     -------
-- more --, next page: Space, continue: g, quit: ^C
```

Command: Show LLDP and LLDP Med Info

Syntax: **show lldp med media-vlan-policy** [<v_0_to_31>]
show lldp med remote-device [interface (<port_type> [<port_list>])]
show lldp neighbors [interface (<port_type> [<v_port_type_list>])]
show lldp statistics [interface (<port_type> [<v_port_type_list>])]

Description: Display the current LLDP neighbors information. The LLDP (Link Layer Discovery Protocol) protocol helps network administrators manage the network and maintain an accurate network topology. LLDP capable devices discover each other by periodically advertising their presence and configuration parameters via messages called Type Length Value (TLV) fields to neighbor devices.

Mode: #

Example 1: Display the **lldp neighbors** and **lldp statistics** command options.

```
# show lldp?
show lldp neighbors [ interface <port_type_list> ]
show lldp statistics [ interface <port_type_list> ]
# show lldp neighbors interface ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
# show lldp statistics
LLDP global counters
Neighbor entries was last changed at 1970-01-01T00:00:00+00:00  (22039 secs. 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
                    Rx      Tx      Rx      Rx       Rx TLV   Rx TLV   Rx TLV
Interface           Frames  Frames  Errors  Discards Errors   Unknown  Organiz.  Aged
---------           ------  ------  ------  -------- ------   -------  --------  ----
GigabitEthernet 1/1    0       0       0       0        0       0        0        0
GigabitEthernet 1/2    0       0       0       0        0       0        0        0
GigabitEthernet 1/3    0       0       0       0        0       0        0        0
GigabitEthernet 1/4    0       0       0       0        0       0        0        0
10GigabitEthernet 1/1  0       0       0       0        0       0        0        0
10GigabitEthernet 1/2  0       0       0       0        0       0        0        0
#
# show lldp statistics
LLDP global counters
Neighbor entries was last changed at 1970-01-01T00:00:21+00:00  (11066 secs. ago
).
Total Neighbors Entries Added    2.
Total Neighbors Entries Deleted  0.
Total Neighbors Entries Dropped  0.
Total Neighbors Entries Aged Out 0.

LLDP local counters
                      Rx          Tx          Rx          Rx          Rx TLV      Rx TLV      Rx TLV
Interface             Frames      Frames      Errors      Discards    Errors      Unknown     Organiz.    Aged
---------             ------      ------      ------      --------    ------      -------     --------    ----
ManagementPort 1/1    0           370         0           0           0           0           0           0
GigabitEthernet 1/1   370         370         0           0           0           0           0           0
GigabitEthernet 1/2   0           0           0           0           0           0           0           0
GigabitEthernet 1/3   370         370         0           0           0           0           0           0
GigabitEthernet 1/4   0           0           0           0           0           0           0           0
GigabitEthernet 1/5   0           0           0           0           0           0           0           0
GigabitEthernet 1/6   0           0           0           0           0           0           0           0
```

Example 2: Display the lldp med command options. LLDP MED (Media Endpoint Discovery) is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

```
# show lldp med ?
    media-vlan-policy    Display media vlan policies.
    remote-device        Display remote device LLDP-MED neighbors information.
# show lldp med media-vlan-policy
Policy Id  Application Type          Tag      Vlan ID  L2 Priority  DSCP
0          Voice                    Tagged   1        0            0
# show lldp med remote-device ?
    |            Output modifiers
    interface
    <cr>
# show lldp med remote-device
No LLDP-MED entries found
# show lldp med remote-device interface ?
    *                    All switches or All ports
    ManagementPort       Management Port
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
# show lldp med remote-device interface
```

Message: *No policies defined*

Message: *No LLDP-MED neighbor information found*
Meaning: LLDP-MED is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices; and as such does not apply to links between LAN infrastructure elements.
Recovery: use LLDP-MED devices or ignore the message.

Command: Show Logging (Syslog)

Syntax: **show logging** <log_id> [switch <switch_list>]
show logging [info] [warning] [error] [switch <switch_list>]

Description: Display the current system log (syslog) information. Syslog is a method to collect messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts which is useful for troubleshooting.
The Syslog data is stored in S4224 RAM by default. Syslog data will be lost with an S4224 reboot unless other provisions are made to save it.

Mode: #

Example: Display the various command options and output.

```
# show logging 1
Switch : 1
ID     : 1
Level  : Informational
Time   : 1970-01-01T00:00:01+00:00
Message:
SYS-BOOTING: Switch just made a cool boot.
# show logging
Switch logging host mode is disabled
Switch logging host address is null
Switch logging level is informational

Number of entries on Switch 1:
Error        : 0
Warning      : 0
Notice       : 5
Informational: 25
All          : 30

ID          Level          Time & Message
----------  -------------  --------------
         1  Informational  1970-01-01T00:00:01+00:00
                           SYS-BOOTING: Switch just made a cool boot.

         2  Notice         1970-01-01T00:00:09+00:00
                           LINK-UPDOWN: Interface GigabitEthernet 1/1, changed
                           state to up.

         3  Notice         1970-01-01T00:01:01+00:00
                           LINK-UPDOWN: Interface Vlan 1, changed state to down
-- more --, next page: Space, continue: g, quit: ^C
# show logging
Switch logging host mode is disabled
Switch logging host address is null
Switch logging level is informational

Number of entries on Switch 1:
Error        : 1
Warning      : 0
Notice       : 4
Informational: 8
```

```
All          : 13

ID          Level          Time & Message
----------  -------------  --------------
         1  Error          1970-01-01T00:00:00+00:00
                           Exception 13 caught at PC 0x806a4bfc - Reserved
                              fffffffe   .v0-v1 0ee60000 00178f40

         2  Informational  1970-01-01T00:00:01+00:00
                           SYS-BOOTING: Switch just made a cool boot.

         3  Notice         1970-01-01T00:00:07+00:00
                           LINK-UPDOWN: Interface Vlan 1, changed state to down
```

Command: Show Loop Protection Configuration

Syntax: **show loop-protect** [**interface** (<port_type> [<plist>])]

Description: Display the current Loop Protection Interface status and configuration. **Note**: STP and Loop Protection may interfere and are not recommended to be enabled on the same physical ports. The parameters are:

<***port_type_list***> List of Port ID (e,g., 1/1,3-5;2/2-4,6).

Mode: #

Example: Display the current Loop Protection Interface status and configuration:

```
# show loop-protect ?
    interface    Interface status and configuration
    <cr>
# show loop-protect

Loop Protection Configuration
=====================================
Loop Protection   : Disable
Transmission Time : 5 sec
Shutdown Time     : 180 sec

GigabitEthernet 1/1
------------------------------
    Loop protect mode is enabled.
    Action is shutdown.
    Transmit mode is enabled.
    No loop.
    The number of loops is 0.
    Status is up.

GigabitEthernet 1/2
------------------------------
    Loop protect mode is enabled.
    Action is shutdown.
    Transmit mode is enabled.
    No loop.
# show loop-protect interface ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
# show loop-protect interface GigabitEthernet ?
    <port_type_list>    Port list in 1/1-4
# show loop-protect interface GigabitEthernet 1/1-4

Loop Protection Configuration
=====================================
Loop Protection   : Disable
Transmission Time : 5 sec
Shutdown Time     : 180 sec

GigabitEthernet 1/1
------------------------------
    Loop protect mode is enabled.
    Action is shutdown.
    Transmit mode is enabled.
    No loop.
    The number of loops is 0.
    Status is up.
```

```
GigabitEthernet 1/2
------------------------------
    Loop protect mode is enabled.
    Action is shutdown.
    Transmit mode is enabled.
    No loop.
-- more --, next page: Space, continue: g, quit: ^C
```

Command: Show Mac Address Table information

Syntax: **show mac address-table** [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>])] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]

Description: Display the current MAC Address table information, including:

| Output modifiers
address MAC address Ingress Frame matching
aging-time Aging time
conf User added static mac addresses
count Total number of mac addresses
interface Select an interface to configure
learning Learn/disable/secure state
static All static mac addresses
vlan Addresses in this VLAN
<***cr***>

Mode: #

Example: Display the various command options and outputs.

```
# show mac address-table ?
    |             Output modifiers
    address       MAC address lookup
    aging-time    Aging time
    conf          User added static mac addresses
    count         Total number of mac addresses
    interface     Select an interface to configure
    learning      Learn/disable/secure state
    static        All static mac addresses
    vlan          Addresses in this VLAN
    <cr>
# show mac address-table
Type    VID  MAC Address        Ports
Dynamic 1    00:c0:f2:56:16:d0  GigabitEthernet 1/1-3
Static  1    00:c0:f2:56:16:d1   CPU
Dynamic 1    00:c0:f2:56:16:d3  GigabitEthernet 1/1-3
Static  1    01:00:0c:cc:cc:cc   CPU
Static  1    01:80:c2:00:00:30   CPU
Static  1    01:80:c2:00:00:38   CPU
Static  1    33:33:00:00:00:01  ManagementPort 1/1 GigabitEthernet 1/1-24 10GbitEthernet 1/1-4 CPU
Static  1    33:33:00:00:00:02  ManagementPort 1/1 GigabitEthernet 1/1-24 10GbitEthernet 1/1-4 CPU
Static  1    33:33:ff:56:16:d0  ManagementPort 1/1 GigabitEthernet 1/1-24 10GbitEthernet 1/1-4 CPU
Static  1    ff:ff:ff:ff:ff:ff  ManagementPort 1/1 GigabitEthernet 1/1-24 10GbitEthernet 1/1-4 CPU
# show mac address-table |
begin    exclude  include
# show mac address-table address 11-22-33-44-55-66
# show mac address-table count
Port                        Dynamic addresses
ManagementPort 1/1               0
GigabitEthernet 1/1              2
GigabitEthernet 1/2              0
GigabitEthernet 1/3              0
GigabitEthernet 1/4              0
GigabitEthernet 1/5              0
GigabitEthernet 1/6              0
GigabitEthernet 1/7              0
GigabitEthernet 1/8              0
GigabitEthernet 1/9              0
GigabitEthernet 1/10             0
GigabitEthernet 1/11             0
GigabitEthernet 1/12             0
GigabitEthernet 1/13             0
```

```
GigabitEthernet 1/14              0
GigabitEthernet 1/15              0
GigabitEthernet 1/16              0
GigabitEthernet 1/17              0
GigabitEthernet 1/18              0
GigabitEthernet 1/19              0
GigabitEthernet 1/20              0
-- more --, next page: Space, continue: g, quit: ^C
# show mac address-table interface ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
# show mac address-table interface *
Type    VID  MAC Address        Ports
Dynamic 1    00:c0:f2:56:16:d0  GigabitEthernet 1/1-3
Dynamic 1    00:c0:f2:56:16:d3  GigabitEthernet 1/1-3
Static  1    33:33:00:00:00:01  ManagementPort 1/1 GigabitEthernet 1/1-24 10Giga
bitEthernet 1/1-4 CPU
Static  1    33:33:00:00:00:02  ManagementPort 1/1 GigabitEthernet 1/1-24 10Giga
bitEthernet 1/1-4 CPU
Static  1    33:33:ff:56:16:d0  ManagementPort 1/1 GigabitEthernet 1/1-24 10Giga
bitEthernet 1/1-4 CPU
Static  1    ff:ff:ff:ff:ff:ff  ManagementPort 1/1 GigabitEthernet 1/1-24 10Giga
bitEthernet 1/1-4 CPU
# show mac address-table learning
Port                Learning
ManagementPort 1/1 Auto
GigabitEthernet 1/1 Auto
GigabitEthernet 1/2 Auto
GigabitEthernet 1/3 Auto
GigabitEthernet 1/4 Auto
GigabitEthernet 1/5 Auto
GigabitEthernet 1/6 Auto
GigabitEthernet 1/7 Auto
GigabitEthernet 1/8 Auto
GigabitEthernet 1/9 Auto
GigabitEthernet 1/10 Auto
GigabitEthernet 1/11 Auto
GigabitEthernet 1/12 Auto
GigabitEthernet 1/13 Auto
GigabitEthernet 1/14 Auto
GigabitEthernet 1/15 Auto
GigabitEthernet 1/16 Auto
GigabitEthernet 1/17 Auto
GigabitEthernet 1/18 Auto
GigabitEthernet 1/19 Auto
GigabitEthernet 1/20 Auto
-- more --, next page: Space, continue: g, quit: ^C
# show mac address-table static
# show mac address-table vlan ?
    <vlan_id>    VLAN IDs 1-4095
# show mac address-table vlan 1
#
```

Command: Show MEP (Maintenance Entity Point) Config

Syntax: **show mep** [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck | pm | syslog | tlv | bfd | rt | lst] [detail]

Description: Display the current MEP (Maintenance Entity End Point) configuration.

|	Output modifiers
<**range_list**>	The range of MEP instances
ais	Show AIS state
aps	Show APS state
bfd	show BFD state
cc	Show CC state
client	Show Client state
detail	Show detailed state including configuration information.
dm	Show DM state
lb	Show LB state
lck	Show LCK state
lm	Show LM state
lst	Show LST state
lt	Show LT state
peer	Show peer mep state
pm	Show PM state
rt	show RT state
syslog	Show Syslog state
tlv	show TLV state
tst	Show TST state
<cr>	Show current MEP State parameters (Fault Causes - defined below).

Mode: #

Example 1: The **show mep** command displays the basic MEP state information.

```
# show mep

MEP state is:
  Inst  cLevel  cMeg  cMep  cAis  cLck cLoop cConf  cSsf  aBlk  aTsf  Peer MEP  cLoc  cRdi cPeriod cPrio
     1   False False False False False False False False False False
     2   False False False False False False False False False False
     3   False False False False False False False False False False
     4   False False False False False False False False False False
     5   False False False False False False False  True False  True

#
```

Example 2: The **show mep detail** command displays the MEP Detail and MEP Basic Configuration:

```
# show mep detail

MEP state is:
  Inst  cLevel  cMeg  cMep  cAis  cLck cLoop cConf  cSsf  aBlk  aTsf  Peer MEP  cLoc  cRdi cPeriod cPrio
     1   False False False False False False False False False False
     2   False False False False False False False False False False
     3   False False False False False False False False False False
     4   False False False False False False False False False False
     5   False False False False False False False  True False  True


MEP Basic Configuration is:
  Inst  Mode  Voe  Vola  Direct                  Port    Dom  Level       Format              Name
Meg id  Mep id   Vid  Flow        Eps
    MAC
     1   Mep              Down    GigabitEthernet 1/1   Port      0      ITU ICC
ICC000MEG0000       1     0     -          0  00-C0-F2-56-1A-91
     2   Mep              Down    GigabitEthernet 1/1   Port      0      ITU IC
C                     ICC000MEG0000       1     0     -          1  00-C0-F2-56-1A-91
-- more --, next page: Space, continue: g, quit: ^C
```

Example 3: The **show mep ais** and **show mep aps** commands:

```
# show mep ais ?
    |                       Output modifiers
    <Inst : range_list>     The range of MEP instances
    detail                  Show detailed state including configuration
                            information.
    <cr>
# show mep ais detail

MEP AIS Configuration is:
     Inst     Period     Protection

# show mep aps ?
    |                       Output modifiers
    <Inst : range_list>     The range of MEP instances
    detail                  Show detailed state including configuration
                            information.
    <cr>
# show mep aps detail

MEP APS Configuration is:
     Inst     Prio     Cast     Type    Octet
        2        7    Multi     laps        1

#
```

Example 4: The **show mep bfd** and **show mep bfd-auth-key** commands:

```
# show mep bfd
BFD not supported
#
```

Example 5: The **show mpe cc** and **show mep client** commands:

```
# show mep cc ?
    |                       Output modifiers
    <Inst : range_list>     The range of MEP instances
    detail                  Show detailed state including configuration
                            information.
    <cr>
# show mep cc detail

MEP CC Configuration is:
     Inst     Prio     Period

# show mep client ?
    |                       Output modifiers
    <Inst : range_list>     The range of MEP instances
    detail                  Show detailed state including configuration
                            information.
    <cr>
# show mep client detail

MEP CLIENT Configuration is:
     Inst     Domain     Client     Flows     AIS Prio     LCK Prio     Level
        1       Port
```

```
        2       Port
        3       Port
        4       Port
#
```

Example 6: The **show mep dm** command:

```
# show mep dm detail ?
    |                     Output modifiers
    <Inst : range_list>   The range of MEP instances
    <cr>
# show mep dm detail

MEP DM state is:

RxTime : Rx Timeout
RxErr :  Rx Error
AvTot :  Average delay Total
AvN :    Average delay last N
Min :    Min Delay value
Max :    Max Delay value
AvVarT : Average delay Variation Total
AvVarN : Average delay Variation last N
MinVar : Min Delay Variation value
MaxVar : Max Delay Variation value
OF  :    Overflow. The number of statistics overflow.

            Inst       Tx       Rx   RxTime    RxErr     AvTot       AvN       M
in      Max  AvVarTot   AvVarN    MinVar   MaxVar  OF Unit
1-Way FtoN     1        0        0        0        0         0         0
 0        0         0        0         0        0   0   us
1-Way NtoF     1        0        0        0        0         0         0
 0        0         0        0         0        0   0   us
-- more --, next page: Space, continue: g, quit: ^C
```

Example 7: The **show mep lb** command:

```
# show mep lb detail
MEP LB state is:
     Inst     Transaction ID     TX LBM                  MAC     Received     Out Of Order
        1                  1          0     00-00-00-00-00-00           0      0
        2                  1          0     00-00-00-00-00-00           0      0
        3                  1          0     00-00-00-00-00-00           0      0


MEP LB Configuration is:
     Inst     Dei     Prio     Cast     Mep                  MAC     ToSend Size     Interval

#
```

Example 8: The **show mep lck, show mep lm**, and **show mep lt** commands:

```
# show mep lck detail

MEP LCK Configuration is:
     Inst     Period

# show mep lm detail

MEP LM state is:
     Inst     Tx     Rx     Near Count     Far Count     Near Ratio     Far Ratio
        1      0      0              0             0              0      0
        2      0      0              0             0              0      0
        3      0      0              0             0              0      0


MEP LM Configuration is:
     Inst     Prio     Cast      Ended     Period     Flr

# show mep lt detail
MEP LT state is:
     Inst     Transaction ID     Ttl     Mode     Direction   Forwarded     relay
Last MAC              Next MAC


MEP LT Configuration is:
     Inst     Prio     Mep                  MAC     Ttl
```

Example 9: The **show mep lst** and **show mep tst** commands:

```
# show mep lst?
    lst     show LST state
    <cr>
# show mep lst ?
    |               Output modifiers
    <range_list>    The range of MEP instances
    detail          Show detailed state including configuration information.
    <cr>
# show mep tst detail
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
        3                  0                  0           0             0


MEP TST Configuration is:
     Inst     Dei     Prio     Mep     rate     Size      Pattern   Sequence   tx       rx

#
```

Example 10: The **show mep peer detail** command:

```
# show mep peer detail ?
    |                     Output modifiers
    <Inst : range_list>   The range of MEP instances
    <cr>
# show mep peer detail

MEP Peer MEP Configuration is:
     Inst     Peer id              Peer MAC
        2           1     10-00-00-00-00-01

#
```

Example 11: The **show mep pm** command:

```
# show mep pm ?
    |               Output modifiers
    <range_list>    The range of MEP instances
    detail          Show detailed state including configuration information.
    <cr>
# show mep pm?
    pm      Show PM state
    <cr>
# show mep pm??
show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck | pm |
syslog | tlv | bfd | rt | lst ] [ detail ]
# show mep pm detail

MEP PM Configuration is:
     Inst  enabled
        1    False
        2    False
        3    False
        4    False

#
```

Example 12: The **show mep rt** command:

```
# show mep rt ?
    |               Output modifiers
    <range_list>    The range of MEP instances
    detail          Show detailed state including configuration information.
    <cr>
# show mep rt
RT not supported
#
```

Example 13: The show mep syslog command:

```
# show mep syslog ?
    |               Output modifiers
    <range_list>    The range of MEP instances
    detail          Show detailed state including configuration information.
    <cr>
# show mep syslog?
    syslog    Show Syslog state
    <cr>
# show mep syslog??
show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck | pm |
syslog | tlv | bfd | rt ] [ detail ]
# show mep syslog detail

MEP Syslog Configuration is:
     Inst  enabled
        1    False
        2    False
        3    False
        4    False

#
```

Example 14: The **show mep tlv** command:

```
# show mep tlv?
    tlv     show TLV state
    <cr>
# show mep tlv ?
    |               Output modifiers
    <range_list>    The range of MEP instances
    detail          Show detailed state including configuration information.
    <cr>
# show mep tlv??
show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck | pm |
syslog | tlv | bfd | rt | lst ] [ detail ]
# show mep tlv

MEP CCM TLV Status is:
     Inst  Peer MEP     OS OUI   OS Sub   OS Value   PS Value   IS Value   OS RX
   PS RX   IS RX
        1
        2
        3
        4

# show mep tlv detail

MEP CCM TLV Status is:
     Inst  Peer MEP     OS OUI   OS Sub   OS Value   PS Value   IS Value   OS RX
   PS RX   IS RX
        1
        2
        3
```

```
        4


MEP TLV Configuration is:
Organization-Specific TLV: OUI 00-00-0C
Organization-Specific TLV: Sub-Type 1
Organization-Specific TLV: Value 2

#
```

Example 15: The **show mep tst state** command:

```
# show mep tst ?
    |               Output modifiers
    <range_list>    The range of MEP instances
    detail          Show detailed state including configuration information.
    <cr>
# show mep tst?
    tst     Show TST state
    <cr>
# show mep tst??
show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck | pm |
syslog | tlv | bfd | rt | lst ] [ detail ]
# show mep tst
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
        3                  0                  0           0             0
        4                  0                  0           0             0
        5                  0                  0           0             0

# show mep tst detail
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
        3                  0                  0           0             0
        4                  0                  0           0             0
        5                  0                  0           0             0


MEP TST Configuration is:
     Inst      Dei     Prio     Mep     rate     Size      Pattern   Sequence    tx       rx

#
```

MEP Detail Configuration Parameters

The MEP State Parameters (Fault Causes) are described below.

Inst: the instance number reporting on.

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. The 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 an 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.

MEP Basic Configuration Parameters

Mode: Mode can be MEP or MIP.

Voe: MEP is VOE enabled (for de-aggregation of VLAN related services (such as VoIP) per EVC on an optical port).

PM: Performance monitoring Data Set collection (MEF35).

Vola: VOE related parameter.

Direct: Direction is Up or Down

Port: MEP Residence Port

Dom: Domain; Domain can be Port, EVC, VLAN, or MPLS Link/Tunnel/PW/LSP.

Level: The MEG level of the MEP.

Format: ITU ICC or IEEE Format.

Name: the Domain Name of the MEP.

Meg id: the Maintenance Entity Group identifier.

Mep id: The Maintenance Entity End point identifier.

Vid: The MEP VLAN ID.

Flow: The related flow instance.

Eps: The related Ethernet Protection Switching instance.

MAC: The related MAC address.

Command: Show Mirror Session Details

Syntax: **show monitor** [session { <session_number> | all | remote }]

Description: Display mirror monitoring details.

Mode: #

Example 1: Display mirror monitoring details:

```
# show monitor??
    monitor    Monitoring different system events
    <cr>
# show monitor ?
    session    MIRROR session
    <cr>
# show monitor session ?
    <1>       MIRROR session number
    all       Show all MIRROR sessions
    remote    Show only Remote MIRROR sessions
# show monitor session 1

Session 1
---------
Mode                      : Disabled
Type                      : Mirror
Source VLAN(s)            :
CPU Port                  :
# show monitor
```

Command: Show MVR (Multicast VLAN Registration) Configuration

Syntax: **show mvr** [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

Description: Display the current Multicast VLAN Registration configuration.
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. 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.

Mode: #

Example 1: Display the various **mvr** command functions:

```
# show mvr?
    mvr     Multicast VLAN Registration configuration
    <cr>
# show mvr ?
    |                 Output modifiers
    detail            Detail information/statistics of MVR group database
    group-database    Multicast group database from MVR
    name              Search by MVR name
    vlan              Search by VLAN
    <cr>
# show mvr?
    mvr     Multicast VLAN Registration configuration
    <cr>
# show mvr?
show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface (
 <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show mvr

MVR is now enabled to start group registration.

Switch-1 MVR-IGMP Interface Status

IGMP MVR VLAN 10 (Name is not set) interface is enabled.
Querier status is IDLE
RX IGMP Query:0 V1Join:0 V2Join:0 V3Join:0 V2Leave:0
TX IGMP Query:0 / (Source) Specific Query:0
Interface Channel Profile: <No Associated Profile>

Switch-1 MVR-MLD Interface Status

MLD MVR VLAN 10 (Name is not set) interface is enabled.
Querier status is IDLE
RX MLD Query:0 V1Report:0 V2Report:0 V1Done:0
TX MLD Query:0 / (Source) Specific Query:0
Interface Channel Profile: <No Associated Profile>
#
```

Example 2: Display the **mvr** command outputs:

```
# show mvr detail

MVR is now enabled to start group registration.

Switch-1 MVR-IGMP Interface Status

IGMP MVR VLAN 10 (Name is not set) interface is enabled.
Querier status is IDLE ( Forced Non-Querier )
Querier Expiry Time: 255 seconds
IGMP address is not set and will use system's IP address of this interface.
Control frames will be sent as Tagged
PRI:0 / RV:2 / QI:125 / QRI:100 / LMQI:5 / URI:1
RX IGMP Query:0 V1Join:0 V2Join:0 V3Join:0 V2Leave:0
TX IGMP Query:0 / (Source) Specific Query:0
IGMP RX Errors:0; Group Registration Count:0
Port Role Setting:
Source Port  : Gi 1/2
Receiver Port: Gi 1/3
Inactive Port: Mgmt 1/1,Gi 1/1,Gi 1/4,Gi 1/5,Gi 1/6,Gi 1/7,Gi 1/8,Gi 1/9,Gi 1/10
,Gi 1/11,Gi 1/12,Gi 1/13,Gi 1/14,Gi 1/15,Gi 1/16,Gi 1/17,Gi 1/18,Gi 1/19,Gi 1/20
,Gi 1/21,Gi 1/22,Gi 1/23,Gi 1/24,10G 1/1,10G 1/2,10G 1/3,10G 1/4
Interface Channel Profile: <No Associated Profile>

Switch-1 MVR-MLD Interface Status

MLD MVR VLAN 10 (Name is not set) interface is enabled.
Querier status is IDLE ( Forced Non-Querier )
Querier Expiry Time: 255 seconds
MLD address will use Link-Local address of this interface.
Control frames will be sent as Tagged
PRI:0 / RV:2 / QI:125 / QRI:100 / LMQI:5 / URI:1
RX MLD Query:0 V1Report:0 V2Report:0 V1Done:0
TX MLD Query:0 / (Source) Specific Query:0
MLD RX Errors:0; Group Registration Count:0
Port Role Setting:
Source Port  : Gi 1/2
Receiver Port: Gi 1/3
Inactive Port: Mgmt 1/1,Gi 1/1,Gi 1/4,Gi 1/5,Gi 1/6,Gi 1/7,Gi 1/8,Gi 1/9,Gi 1/10
,Gi 1/11,Gi 1/12,Gi 1/13,Gi 1/14,Gi 1/15,Gi 1/16,Gi 1/17,Gi 1/18,Gi 1/19,Gi 1/20
,Gi 1/21,Gi 1/22,Gi 1/23,Gi 1/24,10G 1/1,10G 1/2,10G 1/3,10G 1/4
Interface Channel Profile: <No Associated Profile>
```

Messages:

MVR is currently disabled, please enable MVR to start group registration.

W mvr 00:42:15 54/_mvr_vlan_warning_handler#4036: Warning: Please adjust the management VLAN ports overlapped with MVR source ports!

Command: Show NTP (Network Timing Protocol) Config

Syntax: **show ntp status**

Description: Display the current NTP (Network Timing Protocol) configuration. NTP is widely used to synchronize system clocks among a set of distributed time servers and clients. NTP version 4 is implemented. NTP is disabled by default. The NTP IPv4 or IPv6 address can be configured, and a maximum of 5 servers is supported.

Mode: #

Example: Display the current NTP mode and status.

```
# show ntp status
NTP Mode : disabled
Idx   Server IP host address (a.b.c.d) or a host name string
---   ----------------------------------------------------
1     192.168.1.30
2
3
4
5
#
```

Command: Show Performance Monitor Info

Syntax: **show perf-mon interval-info** [id <b_id_number>] [feature { lm | dm | evc }]
show perf-mon { current | interval-id <interval_id> [instance <instance_id>] }
feature { lm | dm | evc }

Description: Display the current Performance Monitor interval information.

Mode: #

Example: Display the various command functions.

```
# show perf-mon ?
    current          Current interval ID
    interval-id      Specific interval
    interval-info    Measurement interval information
# show perf-mon current ?
    feature    Features
# show perf-mon current feature ?
    dm     Delay Measurement
    evc    EVC
    lm     Loss Measurement
# show perf-mon current feature dm ?
    <cr>
# show perf-mon current feature dm
# show perf-mon current feature lm
# show perf-mon current feature evc
# show perf-mon interval-id ?
    <uint>    Interval ID
# show perf-mon interval-id 1 ?
    feature     Features
    instance    MEP or EVC instance
# show perf-mon interval-id 1 feature ?
    dm     Delay Measurement
    evc    EVC
    lm     Loss Measurement
# show perf-mon interval-id 1 feature dm ?
    <cr>
# show perf-mon interval-id 1 feature dm
# show perf-mon interval-info ?
    feature    Features
    id         Measurement interval id
    <cr>
# show perf-mon interval-info feature dm
# show perf-mon interval-info id ?
    <uint>    Measurement interval id
# show perf-mon interval-info id 2 ?
    feature    Features
    <cr>
# show perf-mon interval-info id 2
#
```

Command: Show Platform-specific Information

Syntax: **show platform phy** [interface (<port_type> [<v_port_type_list>])]
show platform phy id [interface (<port_type> [<v_port_type_list>])]
show platform phy instance

Description: Display the current PHY instance, interface, and status information.

Mode: #

Example: Display the various command functions.

```
# show platform phy ?
    |            Output modifiers
    id
    instance     PHY Instance Information
    interface
    mode         Operating mode of PHY
    <cr>
# show platform phy id?
    id
    <cr>
# show platform phy id ?
    |            Output modifiers
    interface
    <cr>
# show platform phy id
Port   Channel    API Base   Phy Id     Phy Rev.
----   -------    --------   -------    ------
29     0          0 (1g)     8221       1
25     1          25 (10g)    8488       5
26     0          25 (10g)    8488       5
27     1          27 (10g)    8488       5
28     0          27 (10g)    8488       5
# show platform phy id interface ?
    *                    All switches or All ports
    ManagementPort       Management Port
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
# show platform phy id interface ManagementPort ?
    |                   Output modifiers
    <port_type_list>    List of Port ID, ex, 1/1,3-5;2/2-4,6
# show platform phy id interface ManagementPort 1/1
Port   Channel    API Base   Phy Id     Phy Rev.
----   -------    --------   -------    ------
29     0          0 (1g)     8221       1
# show platform phy instance
Next Restart    : Cool
Previous Restart: Cool
Current API Version : 1
Previous API Version: 1
Phy Instance Restart Source:1G
Phy Instance Restart Port:0
Current Phy Start Instance:none
# show platform phy interface ?
    *                    All switches or All ports
    ManagementPort       Management Port
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
# show platform phy interface *
Port   API Inst   WAN/LAN/1G Mode       Duplex     Speed      Link
----   ---------  ---------  ----       ------     -----      ----
29     Default    1G         ANEG       -          -          Yes
```

```
25     Default    1G         -          -          -          No
26     Default    1G         -          -          -          No
27     Default    1G         -          -          -          No
28     Default    1G         -          -          -          No
#
# show platform phy ?
    |             Output modifiers
    id
    instance      PHY Instance Information
    interface
    mode          Operating mode of PHY
    <cr>
#
```

Platform-specific Parameters

API Inst: e.g., Default.

WAN/LAN/1G: e.g., **1G**.

Mode: e.g., **PD** or **Forced** mode.

Duplex: e.g., **FDX** (Full Duplex) or **HDX** (Half Duplex) mode.

Speed: e.g., **10M**, **100M** mode.

Link: e.g., **No** or **Yes**.

Issues seen during 1G PHY warmstart: e.g., **No** issues seen during the last 1G PHY restart.

Next Restart: e.g., **Cold** or **Warm** or **Cool**.

Previous Restart: e.g., **Cold** or **Warm** or **Cool**.

Current API Version: e.g., **1**.

Previous API Version: e.g., **0** or **1** .

Phy Instance Restart Source: e.g., **1G**.

Phy Instance Restart Port: e.g., **0**.

Current Phy Start Instance: e.g., **none**.

Command: Show Port Security for a Port

Syntax: **show port-security port** [interface (<port_type> [<v_port_type_list>])]

Description: Display the current MAC Addresses learned by Port Security.

Mode: #

Example: Display the various command options and a sample output.

```
# show port-security port interface?
    interface
# show port-security port interface ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
# show port-security port
GigabitEthernet 1/1
-------------------
MAC Address        VID   State       Added                     Age/Hold Time
-----------------  ----  ----------  ------------------------  -------------
<none>

GigabitEthernet 1/2
-------------------
MAC Address        VID   State       Added                     Age/Hold Time
-----------------  ----  ----------  ------------------------  -------------
<none>

GigabitEthernet 1/3
-------------------
MAC Address        VID   State       Added                     Age/Hold Time
-----------------  ----  ----------  ------------------------  -------------
<none>

GigabitEthernet 1/4
-------------------
MAC Address        VID   State       Added                     Age/Hold Time
-----------------  ----  ----------  ------------------------  -------------
<none>
#
```

Port Security lets you configure the Port Security Limit Control system and port settings. Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken.

System-wide and Port-level configuration parameters are available for configuring the Port Security Limit Control.

The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

Command: Show Port Security for the Switch

Syntax: **show port-security switch** [interface (<port_type> [<v_port_type_list>])]

Description: Display the current port security switch status.

Mode: #

Example: Display the current port security switch status.

```
# show port-security switch interface GigabitEthernet 1/1-4
Users:
L = Limit Control
8 = 802.1X
Interface                Users  State          MAC Cnt
-----------------------  -----  -------------  -------
GigabitEthernet 1/1      --     No users             0
GigabitEthernet 1/2      --     No users             0
GigabitEthernet 1/3      --     No users             0
GigabitEthernet 1/4      --     No users             0
# show port-security switch
GigabitEthernet 1/1      --     No users             0
GigabitEthernet 1/2      --     No users             0
GigabitEthernet 1/3      --     No users             0
GigabitEthernet 1/4      --     No users             0
GigabitEthernet 1/5      --     No users             0
GigabitEthernet 1/6      --     No users             0
GigabitEthernet 1/7      --     No users             0
GigabitEthernet 1/8      --     No users             0
GigabitEthernet 1/9      --     No users             0
GigabitEthernet 1/10     --     No users             0
GigabitEthernet 1/11     --     No users             0
GigabitEthernet 1/12     --     No users             0
GigabitEthernet 1/13     --     No users             0
GigabitEthernet 1/14     --     No users             0
GigabitEthernet 1/15     --     No users             0
GigabitEthernet 1/16     --     No users             0
GigabitEthernet 1/17     --     No users             0
GigabitEthernet 1/18     --     No users             0
GigabitEthernet 1/19     --     No users             0
GigabitEthernet 1/20     --     No users             0
GigabitEthernet 1/21     --     No users             0
GigabitEthernet 1/22     --     No users             0
-- more --, next page: Space, continue: g, quit: ^C
```

Messages: *% No such port: GigabitEthernet 1/7*

Command: Show Privilege Levels

Syntax: **show privilege**

Description: Display the current CLI command privilege levels.

Mode: #

Example 1: Display the command options:

```
# Show privilege | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show privilege | begin ?
    LINE    String to match output lines
# show privilege
#
```

Example 2: Configure a Priv level and then do a 'show priv' command::

```
(config)# privilege config-vlan level 15 ?
    <line128>    Initial valid words and literals of the command to modify, in
                 128 char's
(config)# privilege config-vlan level 15 vlan
(config)# end
# show priv

 ------------------------------------------
|   The order is as the input sequence and   |
|   the last one has the highest priority.   |
 ------------------------------------------

  privilege config-vlan level 15 vlan

#
```

A set of privilege attributes may be assigned to each command based on the level configured.
A command cannot be accessed or executed if the logged in user does not have sufficient privilege.

User EXEC Mode: The initial mode available for the users for the insufficient privileges. The User EXEC mode contains a limited set of commands. The command prompt shown at this level is **>**.

Privileged EXEC Mode: The administrator/user must enter the Privileged EXEC mode in order to have access to the full suite of CLI commands. The Privileged EXEC mode requires password authentication using an 'enable' command if set. The command prompt shown at this level is **#**.

Command: Show Process

Syntax: **show process list** [detail]
show process load
Description: Display the current process list and process load info:
Mode: #
Example 1: Display the current process **list** info:

```
# show process ?
    list    list
    load    load
# show process list
ID  State SetPrio CurPrio Name                    1sec Load 10sec Load Stack Base Size  Used
--- ----- ------- ------- ---------------------- --------- ---------- ---------- ----- -----
DSR N/A       N/A     N/A DSR Context                   N/A        N/A        N/A   N/A   N/A
  2 Run        31      31 Idle Thread                   N/A        N/A 0x82cf5a28  2048  1072
  3 Sleep       6       6 Network alarm support         N/A        N/A 0x835191b8  4096  1928
  4 Sleep       7       7 Network support               N/A        N/A 0x83517018  8192  2472
  5 Susp       15      15 pthread.00000800              N/A        N/A 0x83528e50  7828   292
  6 Sleep       7       7 Main                          N/A        N/A 0x82566978 16384   632
  7 Sleep       7       7 Critd                         N/A        N/A 0x828e8424  8192   772
  8 Sleep       8       8 Configuration                 N/A        N/A 0x80f99ad0  8192  1044
  9 Sleep       7       7 ICFG Loader                   N/A        N/A 0x8123b200 65536 11320
# show process list detail ?
    |       Output modifiers
    <cr>
# show process list detail
Version      : S4224 (standalone) 2.2.0
Build Date   : 2015-05-28T22:12:33-05:00
Warning: Return addresses are highly unreliable (code seems to be compiled with -O2)
ID  State SetPrio CurPrio Name                    1sec Load 10sec Load Stack Base Size  Used
--- ----- ------- ------- ---------------------- --------- ---------- ---------- ----- -----
DSR N/A       N/A     N/A DSR Context                   N/A        N/A        N/A   N/A   N/A
  2 Run        31      31 Idle Thread                   N/A        N/A 0x82cf5a28  2048  1072
#0  0x807477b0
#1  0x80746208
#2  0x80040b30
#3  0x807449a8
#4  0x807449ac
#5  0x80747570
#6  0x807437e4
#7  0x8074586c
#8  0x80745840
-- more --, next page: Space, continue: g, quit: ^C
```

Example 2: Display the current process **load** info:

```
# show process l?
    list    list
    load    load
# show process load?
    load    load
    <cr>
# show process load ?
    <cr>
# show process load
Load average(100ms, 1s, 10s):   0%,   0%,   1%
#
```

Command: Show PTP Precision Time Protocol (IEEE 1588) Config

Syntax: **show ptp** <clockinst> local-clock
show ptp <clockinst> slave-cfg
show ptp <clockinst> slave-table-unicast
show ptp <clockinst> { default | current | parent | time-property | filter | servo | clk | ho | uni | master-table-unicast | slave | { { port-state | port-ds |wireless | foreign-master-record } [interface (<port_type> [<v_port_type_list>])] } }
show ptp ext-clock
show ptp system-time

Description: Display the current IEEE 1588 PTP configuration. 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).
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.

Mode: #

Example 1: Display the various show PTP command capabilities:

```
# show ptp?
    ptp    Precision time Protocol (1588)
# show ptp ?
    <0-3>          Show various PTP data
    ext-clock      Show the external clock configuration.
    system-time    Show the PTP <-> system time synchronization mode.
# show ptp 0 ?
    clk                     Show PTP slave clock options parameters.
    current                 Show PTP current data set (IEEE1588 paragraph 8.2.2).
    default                 Show PTP default data set (IEEE1588 paragraph 8.2.1).
    filter                  Show PTP filter parameters.
    foreign-master-record   Show PTP port foreign masters.
    ho                      Show PTP slave holdover parameters.
    local-clock             Show local clock current time
    master-table-unicast    Show PTP master list of connected unicast slaves.
    parent                  Show PTP parent data set (IEEE1588 paragraph 8.2.3).
    port-ds                 Show PTP port data set (IEEE1588 paragraph 8.2.5).
    port-state              Show PTP port state.
```

```
    servo                    Show PTP servo parameters.
    slave                    Show PTP slave clock lock threshold parameters.
    slave-cfg                Show slave lock configuration
    slave-table-unicast      Show the Unicast slave table of the requested unicast masters
    time-property            Show PTP time properties data set (IEEE1588 paragraph 8.2.4).
    uni                      Show PTP slave unicast configuration parameters.
    wireless                 Show PTP port wireless parameters.
# show ptp 0 clk
Option  threshold  'P'constant
------  ---------  -----------
free     1000       2
# show ptp 0 current ?
    |       Output modifiers
    <cr>
# show ptp 0 current
stpRm  OffsetFromMaster    MeanPathDelay
-----  ------------------  ------------------
0       0.000,000,000       0.000,000,000
# show ptp 0 default
# show ptp 0 default
ClockId  DeviceType  2StepFlag  Ports  vtss_appl_clock_identity     Dom
-------  ----------  ---------  -----  --------------------------  ---
0        BC-frontend False      6      00:c0:f2:ff:fe:56:1a:38      0

vtss_appl_clock_quality         Pri1  Pri2
------------------------------  ----  ----
Cl:251 Ac:Unknwn Va:65535       128   128

Protocol       One-Way    VLAN Tag Enable    VID    PCP
-------------  ---------  -----------------  -----  ---
EthernetMixed  True       True               1      0

Mep Id
--------
1
# show ptp 0 filter
DelayFilter  OffsetFilter  Period  Dist  Height       Percentage   ResetThres
-----------  ------------  ------  ----  -----------  -----------  ----------
6            0             1       2     0            0            0
#
# show ptp 0 foreign-master-record
Port  ForeignmasterIdentity         ForeignmasterClockQality     Pri1  Pri2  Qualif  Best
----  ----------------------------  --------------------------  ----  ----  ------  -----
# show ptp 0 ho
Holdover filter  Adj threshold (ppb)
---------------  -------------------
             60                 30.0
Holdover Ok  Holdover offset (ppb)
-----------  ---------------------
FALSE                         0.0
# show ptp 0 local-clock
PTP Time (0)    : 1970-01-08T01:08:10+00:00 132,538,400
Clock Adjustment method: Internal Timer
```

```
# show ptp 0 master-table-unicast
ip_addr          mac_addr           port  Ann  Sync
---------------  -----------------  ----  ---  -----
# show ptp 0 parent
ParentPortIdentity      port  Pstat  Var  ChangeRate
----------------------  ----  -----  ---  ----------
00:c0:f2:ff:fe:56:1a:38 0     False  0    0

GrandmasterIdentity      GrandmasterClockQuality    Pri1  Pri2
-----------------------  -------------------------  ----  ----
00:c0:f2:ff:fe:56:1a:38  Cl:251 Ac:Unknwn Va:65535  128   128
# show ptp 0 port-ds
Port  Enabled  Stat  MDR  PeerMeanPathDel  Anv  ATo  Syv  SyvErr  Dlm  MPR  Dela
yAsymmetry   IngressLatency   EgressLatency    Ver
----  -------  ----  ---  ---------------  ---  ---  ---  ------  ---  ---  ----
-----------  ---------------  ---------------  ---
1     False    dsbl  3     0.000,000,000   1    3    0    No      p2p  3     0.0
00,000,000    0.000,000,000    0.000,000,000   2
2     True     dsbl  3     0.000,000,000   1    3    0    No      p2p  3     0.0
00,000,000    0.000,000,000    0.000,000,000   2
3     True     dsbl  3     0.000,000,000   1    3    0    No      p2p  3     0.0
00,000,000    0.000,000,000    0.000,000,000   2
4     False    dsbl  3     0.000,000,000   1    3    0    No      p2p  3     0.0
00,000,000    0.000,000,000    0.000,000,000   2
5     False    dsbl  3     0.000,000,000   1    3    0    No      p2p  3     0.0
00,000,000    0.000,000,000    0.000,000,000   2
6     False    dsbl  3     0.000,000,000   1    3    0    No      p2p  3     0.0
00,000,000    0.000,000,000    0.000,000,000   2
# show ptp 0 port-state
Port  Enabled  PTP-State  Internal  Link  Port-Timer  Vlan-forw  Phy-timestamper  Peer-delay
----  -------  ---------  --------  ----  ----------  ---------  ---------------  ----------
   1  FALSE    dsbl       FALSE     Up    OutOfSync   Forward    FALSE            OK
   2  TRUE     dsbl       FALSE     Down  OutOfSync   Discard    TRUE             OK
   3  TRUE     dsbl       FALSE     Down  OutOfSync   Discard    TRUE             OK
   4  FALSE    dsbl       FALSE     Down  OutOfSync   Discard    FALSE            OK
   5  FALSE    dsbl       FALSE     Down  In Sync     Discard    FALSE            OK
   6  FALSE    dsbl       FALSE     Down  In Sync     Discard    FALSE            OK
# show ptp 0 port-state interface 10GigabitEthernet 1/1-2
Port  Enabled  PTP-State  Internal  Link  Port-Timer  Vlan-forw  Phy-timestamper  Peer-delay
----  -------  ---------  --------  ----  ----------  ---------  ---------------  ----------
   5  FALSE    dsbl       FALSE     Down  In Sync     Discard    FALSE            OK
   6  FALSE    dsbl       FALSE     Down  In Sync     Discard    FALSE            OK
# show ptp 0 servo
Display  P-enable  I-enable  D-enable  'P'constant  'I'constant  'D'constant
-------  --------  --------  --------  -----------  -----------  -----------
True     True      True      True      3            80           40
# show ptp 0 slave
Slave port  Slave state    Holdover(ppb)
----------  -------------  -------------
0           FREERUN        N.A.
#
```

```
# show ptp 0 slave-cfg
Stable Offset  Offset Ok      Offset Fail
-------------  -------------  -----------
1000           1000           3000
# show ptp 0 slave-table-unicast
Index  IP-addr      State  MAC-addr          Port  Srcport clock id         Srcport port  Grant
-----  -----------  -----  ----------------  ----  ----------------------  ------------  ------
0      192.168.1.30 IDLE
# show ptp 0 time-property
UtcOffset  Valid  leap59  leap61  TimeTrac  FreqTrac  ptpTimeScale  TimeSource
---------  -----  ------  ------  --------  --------  ------------  ----------
0          False  False   False   False     False     True          160
# show ptp 0 uni
index  duration  ip_address       grant  CommState
-----  --------  ---------------  -----  ---------
0      100       192.168.1.30     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
# show ptp 0 wireless
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  Disabled               0.000           0.000
   5  Disabled               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
  11  Disabled               0.000           0.000
  12  Disabled               0.000           0.000
  13  Disabled               0.000           0.000
  14  Disabled               0.000           0.000
  15  Disabled               0.000           0.000
  16  Disabled               0.000           0.000
  17  Disabled               0.000           0.000
  18  Disabled               0.000           0.000
  19  Disabled               0.000           0.000
  20  Disabled               0.000           0.000
-- more --, next page: Space, continue: g, quit: ^C
```

Example 2: Display the **show ptp ext-clock** command output:

```
# show ptp ext-clock
PTP External One PPS mode: Output, Clock output enabled: False, frequency : 1, Preferred adj
method: LTC frequency
#
```

Example 3: Display the **show ptp system-time** command output:

```
# show ptp system-time
System clock synch mode (No System clock to PTP Sync)
#
```

PTP Parameters

Clock Frequency - Lets you set the Clock Frequency. The valid values are 1 - 25000000 Hz (1 - 25MHz).
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.
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 One Way mode no delay measurements are performed (i.e,. 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.

PTP Servo Parameters

The default clock servo uses a PID regulator to calculate the current clock rate:

OffsetFromMaster/ P constant
+ Integral(OffsetFromMaster)/ I constant
+ Differential OffsetFromMaster)/ D constant =
clockAdjustment

The Proportional–Integral–Derivative 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 depends on the accumulation of past errors, and
D is a prediction of future errors, based on current rate of change.

The PTP Servo parameters are:

<**clockinst**> : The 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.

Command: Show PVLAN (Private VLAN) Config

Syntax: **show pvlan** [<pvlan_list>]
show pvlan isolation [interface (<port_type> [<plist>])]

Description: Display the current PVLAN configuration parameters. Private VLANs are based on the source port mask, and there are 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.

Mode: #

Example: Display the current PVLAN configurations.

```
# show pvlan ?
    <range_list>    PVLAN ID to show configuration for
    isolation       show isolation configuration
    <cr>
# show pvlan
PVLAN ID  Ports
--------  --------------------------------------------------------------------------
1         GigabitEthernet 1/1, GigabitEthernet 1/2, GigabitEthernet 1/3,
          GigabitEthernet 1/4, GigabitEthernet 1/5, GigabitEthernet 1/6,
          GigabitEthernet 1/7, GigabitEthernet 1/8, GigabitEthernet 1/9,
          GigabitEthernet 1/10, GigabitEthernet 1/11, GigabitEthernet 1/12,
          GigabitEthernet 1/13, GigabitEthernet 1/14, GigabitEthernet 1/15,
          GigabitEthernet 1/16, GigabitEthernet 1/17, GigabitEthernet 1/18,
          GigabitEthernet 1/19, GigabitEthernet 1/20, GigabitEthernet 1/21,
          GigabitEthernet 1/22, GigabitEthernet 1/23, GigabitEthernet 1/24,
          10GigabitEthernet 1/1, 10GigabitEthernet 1/2, 10GigabitEthernet 1/3,
          10GigabitEthernet 1/4
# show pvlan 2
% None of the requested PVLANs are configured
# show pvlan isolation ?
    interface    List of port type and port ID, ex, Fast 1/1 Gigabit 2/3-5
                 Gigabit 3/2-4 Tengigabit 4/6
    <cr>
```

Messages: *Invalid PVLAN detected*

% None of the requested PVLANs are configured

Command: Show PVLAN Isolation Config

Syntax: **show pvlan isolation** [interface (<port_type> [<plist>])]
<cr>

Description: Display the current Private VLAN isolation interface. In a Private VLAN, communication between isolated ports in that private VLAN is not permitted. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical. The valid range for Port Isolation is all available physical ports By default, No ports are selected for Isolation.

Mode: #

Example:

```
# show pvlan ?
    <range_list>    PVLAN ID to show configuration for.
    isolation       Show isolation configuration.
    <cr>
# show pvlan isolation ?
    interface    List of port type and port ID, ex, Fast 1/1 Gigabit 2/3-5
                 Gigabit 3/2-4 Tengigabit 4/6
    <cr>
# show pvlan isolation
Port                              Isolation
--------------------------------  ---------
GigabitEthernet 1/1               Disabled
GigabitEthernet 1/2               Disabled
GigabitEthernet 1/3               Disabled
GigabitEthernet 1/4               Disabled
GigabitEthernet 1/5               Disabled
GigabitEthernet 1/6               Disabled
GigabitEthernet 1/7               Disabled
GigabitEthernet 1/8               Disabled
GigabitEthernet 1/9               Disabled
GigabitEthernet 1/10              Disabled
GigabitEthernet 1/11              Disabled
GigabitEthernet 1/12              Disabled
GigabitEthernet 1/13              Disabled
GigabitEthernet 1/14              Disabled
GigabitEthernet 1/15              Disabled
GigabitEthernet 1/16              Disabled
GigabitEthernet 1/17              Disabled
GigabitEthernet 1/18              Disabled
GigabitEthernet 1/19              Disabled
GigabitEthernet 1/20              Disabled
# show pvlan isolation interface ?
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
# show pvlan isolation interface 10GigabitEthernet 1/24-26
% No such interface: 10GigabitEthernet 1/24

#
```

Command: Show QoS (Quality of Service)

Syntax: **show qos** [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

Description: Display the current QoS (Quality of Service) parameters for:

| : Output modifiers.
interface: Interface.
maps : Global QoS Maps/Tables.
qce : QoS Control Entry.
storm : Storm policer.
wred : Weighted Random Early Discard.
<cr> : Displays the complete QoS configuration.

Mode: #

Example 1: Display the various commands and configure QoS parameters:

```
# show qos
interface GigabitEthernet 1/1
 qos cos 0
 qos pcp 0
 qos dpl 0
 qos dei 0
 qos trust tag disabled
 qos map tag-cos pcp 0 dei 0 cos 1 dpl 0
 qos map tag-cos pcp 0 dei 1 cos 1 dpl 1
 qos map tag-cos pcp 1 dei 0 cos 0 dpl 0
 qos map tag-cos pcp 1 dei 1 cos 0 dpl 1
 qos map tag-cos pcp 2 dei 0 cos 2 dpl 0
 qos map tag-cos pcp 2 dei 1 cos 2 dpl 1
 qos map tag-cos pcp 3 dei 0 cos 3 dpl 0
 qos map tag-cos pcp 3 dei 1 cos 3 dpl 1
 qos map tag-cos pcp 4 dei 0 cos 4 dpl 0
 qos map tag-cos pcp 4 dei 1 cos 4 dpl 1
 qos map tag-cos pcp 5 dei 0 cos 5 dpl 0
 qos map tag-cos pcp 5 dei 1 cos 5 dpl 1
 qos map tag-cos pcp 6 dei 0 cos 6 dpl 0
 qos map tag-cos pcp 6 dei 1 cos 6 dpl 1
 qos map tag-cos pcp 7 dei 0 cos 7 dpl 0
 qos map tag-cos pcp 7 dei 1 cos 7 dpl 1
-- more --, next page: Space, continue: g, quit: ^C
# show qos ?
    |            Output modifiers
    interface    Interface
    maps         Global QoS Maps/Tables
    qce          QoS Control Entry
    storm        Storm policer
    wred         Weighted Random Early Discard
    <cr>
# show qos | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
```

Example 2: Display the QoS interface parameters:

```
# show qos interface ?
    |                   Output modifiers
    *                   All switches or All ports
    ManagementPort      Management Port
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
    <cr>
```

Example 3: Display the QoS maps options and show the current QoS maps config:

```
# show qos maps ?
    |                           Output modifiers
    cos-dscp                    Map for cos to dscp
    dscp-classify               Map for dscp classify enable
    dscp-cos                    Map for dscp to cos
    dscp-egress-translation     Map for dscp egress translation
    dscp-ingress-translation    Map for dscp ingress translation
    <cr>
# show qos maps
qos map dscp-cos:
=================
DSCP       Trust     Cos  Dpl
---------  --------  ---  ---
0  (BE)    disabled  0    0
1          disabled  0    0
2          disabled  0    0
3          disabled  0    0
4          disabled  0    0
5          disabled  0    0
6          disabled  0    0
7          disabled  0    0
8  (CS1)   disabled  0    0
9          disabled  0    0
10 (AF11)  disabled  0    0
11         disabled  0    0
12 (AF12)  disabled  0    0
13         disabled  0    0
14 (AF13)  disabled  0    0
15         disabled  0    0
16 (CS2)   disabled  0    0
17         disabled  0    0
-- more --, next page: Space, continue: g, quit: ^C
```

Example 4: Display the QCE (QoS Control Entry) config:

```
# show qos qce

static qce 1:
=============
 port: 2-6
 key parameters:
  dmac: any
  smac: any
  tag:
   type: any
   vid: any
   pcp: any
   dei: any
  inner tag:
   type: any
   vid: any
```

```
   pcp: any
   dei: any
  frametype: any
 action parameters:
  cos: 0
  dpl: default
  dscp: default
-- more --, next page: Space, continue: g, quit: ^C
```

Example 5: Display the current QoS WRED (Weighted Random Early Discard) config:

```
# show qos wred ?
    |       Output modifiers
    <cr>
# show qos wred
qos wred:
=========
Queue  Mode      Min Th  Mdp 1  Mdp 2  Mdp 3
-----  --------  ------  -----  -----  -----
    0  disabled      0      1      5     10
    1  disabled      0      1      5     10
    2  disabled      0      1      5     10
    3  disabled      0      1      5     10
    4  disabled      0      1      5     10
    5  disabled      0      1      5     10
#
```

QCL and QCE Configuration

The QCL Configuration is a table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects. A QoS class is associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority.

Frames can be classified by one of four different QoS classes ("Low", "Normal", "Medium", and "High)" for individual application.

Command: Show RADIUS Configuration

Syntax: **show radius-server** [statistics]

Description: Display the current RADIUS configuration parameters.

Mode: #

Example: Display the current RADIUS Server config and statistics:

```
# show radius-server
Global RADIUS Server Timeout      : 5 seconds
Global RADIUS Server Retransmit   : 3 times
Global RADIUS Server Deadtime     : 0 minutes
Global RADIUS Server Key          : Buffrey1
Global RADIUS Server Attribute 4  : 192.168.1.30
Global RADIUS Server Attribute 95 :
Global RADIUS Server Attribute 32 :
RADIUS Server #1:
  Host name  : TestRad-1
  Auth port  : 1812
  Acct port  : 1813
  Timeout    : 9 seconds
  Retransmit : 9 times
  Key        : Buffrey1
# show radius-server statistics
Global RADIUS Server Timeout      : 5 seconds
Global RADIUS Server Retransmit   : 3 times
Global RADIUS Server Deadtime     : 0 minutes
Global RADIUS Server Key          : Buffrey1
Global RADIUS Server Attribute 4  : 192.168.1.30
Global RADIUS Server Attribute 95 :
Global RADIUS Server Attribute 32 :
RADIUS Server #1:
  Host name  : TestRad-1
  Auth port  : 1812
  Acct port  : 1813
  Timeout    : 9 seconds
  Retransmit : 9 times
  Key        : Buffrey1

RADIUS Server #1 (0.0.0.0:1812) 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:                          Ready
Round-Trip Time:                    0 ms

RADIUS Server #1 (0.0.0.0:1813) 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:                          Ready
Round-Trip Time:                    0 ms
# show radius-server
```

Command: Show RMON

Syntax: **show rmon**

Description: Display the current Remote Monitoring configuration. The S4224 RMON (Remote Network Monitoring) function supports the monitoring and protocol analysis of a LAN per IETF RFC 1271. A part of SNMP, RMON is a network management protocol that gathers remote network information. RMON collects nine kinds of information, including packets sent, bytes sent, packets dropped, statistics by host, by conversations between two sets of addresses, and certain kinds of events that occurred. A network administrator can find out how much bandwidth or traffic each user is imposing on the network and what web sites are being accessed. Alarms can be set to alert you of impending problems. RMON is designed for "flow-based" monitoring. The parameters are:

- ***alarm*** : Display the RMON alarm table.
- ***event*** : Display the RMON event table.
- ***history*** : Display the RMON history table.
- ***statistics*** : Display the RMON statistics table.

Mode: (config)

Example: Display the **show rmon** command variables:

```
# show rmon ?
    alarm         Display the RMON alarm table
    event         Display the RMON event table
    history       Display the RMON history table
    statistics    Display the RMON statistics table
# show rmon alarm

Alarm ID :     1
----------------
      Interval          : 30
      Variable          : .1.3.6.1.2.1.2.2.1.10.2
      SampleType        : deltaValue
      Value         : 0
      Startup           : risingOrFallingAlarm
      RisingThrld       : 4
      FallingThrld      : 2
      RisingEventIndex  : 4
      FallingEventIndex : 1
# show rmon event

Event ID :     1
----------------
      Description     : rEvent-1
      Type            : logandtrap
      Community       : public
      LastSent        : Never
# show rmon history

History ID :     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
# show rmon statistics

Statistics ID :     1
---------------------
    Data Source : .1.3.6.1.2.1.2.2.1.1.1
    etherStatsDropEvents          : 0
    etherStatsOctets              : 0
```

```
    etherStatsPkts                : 0
    etherStatsBroadcastPkts       : 0
    etherStatsMulticastPkts       : 0
    etherStatsCRCAlignErrors      : 0
    etherStatsUndersizePkts       : 0
    etherStatsOversizePkts        : 0
    etherStatsFragments           : 0
    etherStatsJabbers             : 0
    etherStatsCollisions          : 0
    etherStatsPkts64Octets        : 0
    etherStatsPkts65to127Octets   : 0
    etherStatsPkts128to255Octets  : 0
    etherStatsPkts256to511Octets  : 0
    etherStatsPkts512to1023Octets : 0
    etherStatsPkts1024to1518Octets: 0
#
```

Command: Show Running Configuration

Syntax: **show running-config** [all-defaults]
show running-config feature <feature_name> [all-defaults]
show running-config interface (<port_type> [<list>]) [all-defaults]
show running-config interface vlan <list> [all-defaults]
show running-config line { console | vty } <list> [all-defaults]
show running-config vlan <list> [all-defaults]

Description: Display the current running system information. The current device configuration can be displayed in the form of a virtual file containing the full set of commands necessary to create an identical configuration (with a few exceptions; certain items, such as private SSH keys, are not displayed). This file is called '**running-config'** and is ephemeral by nature; it does not survive across reboots. So it is necessary to save the 'running-config' to FLASH storage under the name 'startup-config' – this file is read and executed upon every boot and is therefore responsible for restoring the running configuration of the system to the state it had when the saving took place.
The 'running-config' can be displayed with this command (some details edited out for brevity; also, the set of interfaces depends on the hardware capabilities).
The parameters are:

|	Output modifiers
all-defaults	Include most/all default values
feature	Show configuration for specific feature.
interface	Show specific interface(s).
line	Show line settings (Console / VTY).
vlan	VLAN list.
<cr>	

Note: Lines that begin with '!' are comments. The file begins with the 'hostname' command and the password for user 'admin', then followed by VLANs 1 and 42. Other configuration may display, such as Spanning Tree Protocol (STP). Then follows a list of all port interfaces on the device, ordered by switch ID, type and port number. All interfaces except GigabitEthernet 1/1 are at default settings, so nothing is displayed for them. This is a general rule of thumb: Only non-default configuration is displayed; otherwise the output would be huge and readability would suffer. There are exceptions, though, to be discussed later. After the physical interfaces follows VLAN interfaces, 1 and 42. Only the latter has an IP address assigned. Finally follows the 'line' section; it specifies characteristics for the serial console ('line console 0') or network CLI management connections ('line vty x'). The configuration as displayed below is what is saved to 'startup-config':

Example 1:

```
# show running-config
Building configuration...
hostname w
logging on
username admin privilege 15 password none
access management
evc 1 vid 1 learning
!
vlan 1
 name default
!
!
ipmc profile range
!
ip route 0.0.0.0 0.0.0.0 192.168.1.10
mvr
ip dhcp relay information option
ip dhcp relay information policy replace
ntp server 1 ip-address 192.168.1.30
```

```
aggregation mode
spanning-tree mst name 00-c0-f2-21-db-83 revision 0
-- more --, next page: Space, continue: g, quit: ^C
```

Example 2:

```
# show running-config
Building configuration...
username admin privilege 15 password none
ip dhcp server
ip dhcp excluded-address 123.4.56.7 124.4.56.8
evc policer 1 enable type single mode aware
evc policer 2 enable cir 10 cbs 10 eir 10 ebs 10
evc policer 3 enable mode coupled cir 10 cbs 10 eir 10 ebs 10
evc policer 20 type single
!
vlan 1
!
!
!
ip dhcp snooping
ip dhcp relay
ip helper-address 192.168.1.30
ip dhcp relay information option
ip dhcp relay information policy replace
spanning-tree mst name 00-c0-f2-56-16-d0 revision 0
ptp 0 mode boundary twostep ethernet twoway id 00:c0:f2:ff:fe:56:16:d0 vid 1 0
ptp 0 time-property utc-offset 0 ptptimescale time-source 160
ptp 0 filter delay 6 period 1 dist 2
ptp 1 mode p2ptransparent twostep ethernet twoway id 00:c0:f2:ff:fe:56:16:d0 vid
 1 0
ptp 1 time-property utc-offset 0 ptptimescale time-source 160
ptp 1 filter delay 6 period 1 dist 2
ptp 2 mode e2etransparent twostep ethernet twoway id 00:00:00:ff:fe:00:00:00 vid
 1 0
ptp 2 time-property utc-offset 0 ptptimescale time-source 160
ptp 2 filter delay 6 period 1 dist 2
ptp 3 mode bcfrontend onestep ethernet oneway id 00:c0:f2:ff:fe:56:16:d0 vid 1 0

ptp 3 time-property utc-offset 0 ptptimescale time-source 160
ptp 3 filter delay 6 period 1 dist 2
!
interface GigabitEthernet 1/1
 no ip dhcp forwarding
!
interface GigabitEthernet 1/2
 ptp 0
 ptp 0 announce interval 1 timeout 3
 ptp 0 sync-interval 0
 ptp 0 delay-mechanism e2e
 ptp 0 delay-req interval 3
 ptp 0 delay-asymmetry 0
-- more --, next page: Space, continue: g, quit: ^C
```

Example 2: Display the current (running) config for a feature.

```
# show running-config feature ?
    <cword>    Valid words are 'GVRP' 'access' 'access-list' 'aggregation'
               'arp-inspection' 'auth' 'clock' 'ddmi' 'dhcp' 'dhcp-snooping'
               'dhcp6_client_interface' 'dhcp_server' 'dns' 'dot1x' 'eps'
               'erps' 'ethersat' 'evc' 'green-ethernet' 'http' 'icli'
               'ip-igmp-snooping' 'ip-igmp-snooping-port'
               'ip-igmp-snooping-vlan' 'ipmc-profile' 'ipmc-profile-range'
               'ipv4' 'ipv6' 'ipv6-mld-snooping' 'ipv6-mld-snooping-port'
               'ipv6-mld-snooping-vlan' 'lacp' 'link-oam' 'lldp' 'logging'
               'loop-protect' 'mac' 'mep' 'mstp' 'mvr' 'mvr-port' 'ntp'
               'perf-mon' 'phy' 'port' 'port-security' 'ptp' 'pvlan' 'qos'
               'rmon' 'snmp' 'source-guard' 'ssh' 'udld' 'user' 'vlan'
               'vtss-rmirror' 'web-privilege-group-level'
# show running-config interface ?
    *                    All switches or All ports
    ManagementPort       Management Port
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
    vlan                 VLAN
# show running-config interface GigabitEthernet ?
    <port_type_list>    Port list in 1/1-4
# show running-config interface GigabitEthernet 1/1
Building configuration...
interface GigabitEthernet 1/1
 no pvlan 1
 pvlan 2
!
end
# show running-config line ?
    console    Console
    vty        VTY
# show running-config vlan ?
    <vlan_list>    List of VLAN numbers
# show running-config vlan 1
Building configuration...
vlan 1
!
end
#
```

Example 3: Show running config for the iCLI feature and include most/all default values.

```
# show running-config feature icli
Building configuration...
!
vlan 1
!
!
!
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
!
interface GigabitEthernet 1/4
!
```

```
interface 10GigabitEthernet 1/1
!
interface 10GigabitEthernet 1/2
!
interface vlan 1
!
!
spanning-tree aggregation
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
!
end
#
```

Command: Show SNMP Config

Syntax: **show snmp <cr>**
show snmp access [<group_name> { v1 | v2c | v3 | any } { auth | noauth | priv }]
show snmp community v3 [<community>]
show snmp host [<conf_name>] [system] [switch] [interface] [aaa]
show snmp mib context
show snmp mib ifmib ifIndex
show snmp security-to-group [{ v1 | v2c | v3 } <security_name>]
show snmp user [<username> <engineID>]
show snmp view [<view_name> <oid_subtree>]

Description: Display the current SNMP info (access, community, host, MIB, security, user, and view). The parameters are:

|	Output modifiers
access	access configuration
community	Community
host	Set SNMP host's configurations
mib	MIB(Management Information Base)
security-to-group	Security-to-group configuration
user	User
view	MIB view configuration
<cr>	Display all of the current SNMP config parameters.

Mode: #

Example 1: The **show snmp** (show all) command:

```
# show snmp

SNMP Configuration
SNMP Mode                     : enabled
SNMP Version                  : 2c
Read Community                : public
Write Community               : private
Trap Mode                     : disabled

SNMPv3 Communities Table:
Community   : public
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0

Community   : private
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0


SNMPv3 Users Table:
User Name               : default_user
Engine ID               : 800007e5017f000001
Security Level          : NoAuth, NoPriv
Authentication Protocol : None
Privacy Protocol        : None


SNMPv3 Groups Table;
Security Model : v1
Security Name  : public
Group Name     : default_ro_group

Security Model : v1
```

```
Security Name  : private
Group Name     : default_rw_group

Security Model : v2c
Security Name  : public
Group Name     : default_ro_group

Security Model : v2c
Security Name  : private
Group Name     : default_rw_group

Security Model : v3
Security Name  : default_user
Group Name     : default_rw_group


SNMPv3 Accesses Table:
Group Name       : default_ro_group
Security Model   : any
Security Level   : NoAuth, NoPriv
Read View Name   : default_view
Write View Name  : <no writeview specified>

Group Name       : default_rw_group
Security Model   : any
Security Level   : NoAuth, NoPriv
Read View Name   : default_view
Write View Name  : default_view


SNMPv3 Views Table:
View Name   : default_view
OID Subtree : .1
View Type   : included
```

Example 2: Display the current SNMP server configuration parameters.

```
# show snmp ?
    |                     Output modifiers
    access                access configuration
    community             Community
    host                  Set SNMP host's configurations
    mib                   MIB(Management Information Base)
    security-to-group     security-to-group configuration
    user                  User
    view                  MIB view configuration
    <cr>
# show snmp | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show snmp access ?
    |                         Output modifiers
    <GroupName : word32>      group name
    <cr>
# show snmp access?
    access    access configuration
    <cr>
# show snmp access w ?
    any    any security model
```

```
    v1     v1 security model
    v2c    v2c security model
    v3     v3 security model
# show snmp access w any ?
    auth      authNoPriv Security Level
    noauth    noAuthNoPriv Security Level
    priv      authPriv Security Level
# show snmp access w any auth ?
    |       Output modifiers
    <cr>
# show snmp access w any auth
# show snmp community ?
    v3    SNMPv3
# show snmp community v3 ?
    |                        Output modifiers
    <Community : word32>     Specify community name
    <cr>
# show snmp community v3
Community   : public
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0

Community   : private
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0
```

Example 3: Display the current SNMP host and MIB parameters.

```
# show snmp host ?
    |                       Output modifiers
    <ConfName : word32>     Name of the host configuration
    aaa                     AAA event group
    interface               Interface event group
    switch                  Switch event group
    system                  System event group
    <cr>
# show snmp host
Trap Global Mode: enabled
Trap SnmpTrapHost1 (ID:0) is enabled
Community       : Public
Destination Host: 192.168.1.30
UDP Port        : 162
Version         : V3
Inform Mode     : enabled
Inform Timeout  : 3
Inform Retry    : 5
Probe Mode      : enabled
Engine ID       :
Security Name   : None

# show snmp mib ?
    context    MIB context
    ifmib      IF-MIB
# show snmp mib ifmib ?
    ifIndex    The IfIndex that is defined in IF-MIB
# show snmp mib ifmib?
    ifmib    IF-MIB
# show snmp mib ifmib?
show snmp mib ifmib ifIndex
# show snmp mib ifmib?
    ifmib    IF-MIB
```

```
# show snmp mib ?
    context    MIB context
    ifmib      IF-MIB
# show snmp security-to-group ?
    |        Output modifiers
    v1       v1 security model
    v2c      v2c security model
    v3       v3 security model
    <cr>
# show snmp security-to-group v2c ?
    <SecurityName : word32>    security group name
# show snmp user ?
    |                       Output modifiers
    <Username : word32>     Security user name
    <cr>
# show snmp user w ?
    <Engiedid : word10-32>    Security Engine ID
# show snmp user w e
<Engiedid : word10-32>
# show snmp user
User Name               : default_user
Engine ID               : 800007e5017f000001
Security Level          : NoAuth, NoPriv
Authentication Protocol : None
Privacy Protocol        : None

# show snmp view ?
    |                       Output modifiers
    <ViewName : word32>     MIB view name
    <cr>
# show snmp view
View Name   : default_view
OID Subtree : .1
View Type   : included

#
```

Example 4: Display the current SNMP MIB context. Contexts are an SNMPv3 mechanism where an agent can support parallel versions of the same MIB objects, referring to different underlying data sets. By default, MIB module registrations will use the default empty context of "". It is also possible to provide MIB information using a different (non-default) context.

```
# show snmp mib context
BRIDGE-MIB :
    - dot1dBase (.1.3.6.1.2.1.17.1)
    - dot1dTp (.1.3.6.1.2.1.17.4)
Dot3-OAM-MIB :
    - dot3OamMIB (.1.3.6.1.2.1.158)
EtherLike-MIB :
    - transmission (.1.3.6.1.2.1.10)
IEEE8021-BRIDGE-MIB :
    - ieee8021BridgeBasePortTable (.1.3.111.2.802.1.1.2.1.1.4)
IEEE8021-PAE-MIB :
    - ieee8021paeMIB (.1.0.8802.1.1.1.1)
IEEE8021-Q-BRIDGE-MIB :
    - ieee8021QBridgeMib (.1.3.111.2.802.1.1.4)
IEEE8023-LAG-MIB :
    - lagMIBObjects (.1.2.840.10006.300.43.1)
IF-MIB :
    - ifMIB (.1.3.6.1.2.1.31)
IP-FORWARD-MIB :
```

```
    - ipForward (.1.3.6.1.2.1.4.24)
IP-MIB :
    - ipv4InterfaceTable (.1.3.6.1.2.1.4.28)
    - ipv6InterfaceTable (.1.3.6.1.2.1.4.30)
    - ipTrafficStats (.1.3.6.1.2.1.4.31)
    - ipAddressTable (.1.3.6.1.2.1.4.34)
    - ipNetToPhysicalTable (.1.3.6.1.2.1.4.35)
    - ipv6ScopeZoneIndexTable (.1.3.6.1.2.1.4.36)
    - ipDefaultRouterTable (.1.3.6.1.2.1.4.37)
    - icmpStatsTable (.1.3.6.1.2.1.5.29)
    - icmpMsgStatsTable (.1.3.6.1.2.1.5.30)
LLDP-EXT-MED-MIB :
    - lldpXMedMIB (.1.0.8802.1.1.2.1.5.4795.1)
LLDP-MIB :
    - lldpObjects (.1.0.8802.1.1.2.1)
MAU-MIB :
    - snmpDot3MauMgt (.1.3.6.1.2.1.26)
MGMD-MIB :
    - mgmdMIBObjects (.1.3.6.1.2.1.185.1)
P-BRIDGE-MIB :
    - pBridgeMIB (.1.3.6.1.2.1.17.6)
Q-BRIDGE-MIB :
    - qBridgeMIB (.1.3.6.1.2.1.17.7)
RADIUS-ACC-CLIENT-MIB :
    - radiusAccClientMIBObjects (.1.3.6.1.2.1.67.2.2.1)
RADIUS-AUTH-CLIENT-MIB :
    - radiusAuthClientMIBObjects (.1.3.6.1.2.1.67.1.2.1)
RFC1213-MIB :
    - system (.1.3.6.1.2.1.1)
    - interfaces (.1.3.6.1.2.1.2)
    - ip (.1.3.6.1.2.1.4)
    - snmp (.1.3.6.1.2.1.5)
    - tcp (.1.3.6.1.2.1.6)
    - udp (.1.3.6.1.2.1.7)
RMON-MIB :
    - statistics (.1.3.6.1.2.1.16.1)
    - history (.1.3.6.1.2.1.16.2)
    - alarm (.1.3.6.1.2.1.16.3)
    - event (.1.3.6.1.2.1.16.9)
SFLOW-MIB :
    - sFlowAgent (.1.3.6.1.4.1.14706.1.1)
SMON-MIB :
    - switchRMON (.1.3.6.1.2.1.16.22)
SNMP-FRAMEWORK-MIB :
    - snmpEngine (.1.3.6.1.6.3.10.2.1)
SNMP-MPD-MIB :
    - dot1dTpHCPortTable (.1.3.6.1.2.1.17.4.5)
    - snmpMPDStats (.1.3.6.1.6.3.11.2.1)
SNMP-USER-BASED-SM-MIB :
    - usmStats (.1.3.6.1.6.3.15.1.1)
    - usmUserTable (.1.3.6.1.6.3.15.1.2)
#
```

Example 54: Display the current IfIndex that is defined in IF-MIB:

```
# show snmp mib ?
    context    MIB context
    ifmib      IF-MIB
# show snmp mib ifmib ?
    ifIndex    The IfIndex that is defined in IF-MIB
# show snmp mib ifmib ifIndex ?
    |        Output modifiers
    <cr>
# show snmp mib ifmib ifIndex
ifIndex     ifDescr                                 Interface
----------  --------------------------------------  ---------
         1  VLAN    1                               vlan 1
   1000001  Switch  1 - Port  1                     GigabitEthernet 1/1
   1000002  Switch  1 - Port  2                     GigabitEthernet 1/2
   1000003  Switch  1 - Port  3                     GigabitEthernet 1/3
   1000004  Switch  1 - Port  4                     GigabitEthernet 1/4
   1000005  Switch  1 - Port  5                     GigabitEthernet 1/5
   1000006  Switch  1 - Port  6                     GigabitEthernet 1/6
   1000007  Switch  1 - Port  7                     GigabitEthernet 1/7
   1000008  Switch  1 - Port  8                     GigabitEthernet 1/8
   1000009  Switch  1 - Port  9                     GigabitEthernet 1/9
   1000010  Switch  1 - Port 10                     GigabitEthernet 1/10
   1000011  Switch  1 - Port 11                     GigabitEthernet 1/11
   1000012  Switch  1 - Port 12                     GigabitEthernet 1/12
   1000013  Switch  1 - Port 13                     GigabitEthernet 1/13
   1000014  Switch  1 - Port 14                     GigabitEthernet 1/14
   1000015  Switch  1 - Port 15                     GigabitEthernet 1/15
   1000016  Switch  1 - Port 16                     GigabitEthernet 1/16
   1000017  Switch  1 - Port 17                     GigabitEthernet 1/17
   1000018  Switch  1 - Port 18                     GigabitEthernet 1/18
   1000019  Switch  1 - Port 19                     GigabitEthernet 1/19
-- more --, next page: Space, continue: g, quit: ^C
```

Example 6: Display the current SNMP host parameters.

```
# show snmp host ?
    |            Output modifiers
    <word32>     Name of the host configuration
    aaa          AAA event group
    interface    Interface event group
    switch       Switch event group
    system       System event group
    <cr>
# show snmp host | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show snmp host aaa
Trap Global Mode: Disabled
Trap TestTrp-1 (ID:0) is Disabled
Community       : public
Destination Host: 192.168.1.30
UDP Port        : 162
Version         : V3
Inform Mode     : Enabled
Inform Timeout  : 3
Inform Retry    : 5
Probe Mode      : Disabled
Engine ID       :
Security Name   : None
```

```
Authentication Fail: Enabled
# show snmp host interface
Trap Global Mode: Enabled
Trap 222 (ID:0) is Enabled
Community       : public
Destination Host: 192.168.1.30
UDP Port        : 162
Version         : V3
Inform Mode     : Enabled
Inform Timeout  : 3
Inform Retry    : 5
Probe Mode      : Enabled
Engine ID       :
Security Name   : None
GigabitEthernet   1/1  Link Up    : Enabled
GigabitEthernet   1/2  Link Up    : Enabled
GigabitEthernet   1/3  Link Up    : Enabled
GigabitEthernet   1/4  Link Up    : Enabled
10GigabitEthernet 1/1  Link Up    : Enabled
10GigabitEthernet 1/2  Link Up    : Enabled
GigabitEthernet   1/1  Link Down  : Enabled
GigabitEthernet   1/2  Link Down  : Enabled
GigabitEthernet   1/3  Link Down  : Enabled
GigabitEthernet   1/4  Link Down  : Enabled
10GigabitEthernet 1/1  Link Down  : Enabled
10GigabitEthernet 1/2  Link Down  : Enabled
GigabitEthernet   1/1  LLDP       : Enabled
GigabitEthernet   1/2  LLDP       : Enabled
GigabitEthernet   1/3  LLDP       : Enabled
GigabitEthernet   1/4  LLDP       : Enabled
10GigabitEthernet 1/1  LLDP       : Enabled
10GigabitEthernet 1/2  LLDP       : Enabled
# show snmp host switch
Trap Global Mode: disabled
Trap TestTrp-1 (ID:0) is disabled
Community       : public
Destination Host: 192.168.1.30
UDP Port        : 162
Version         : V3
Inform Mode     : Enabled
Inform Timeout  : 3
Inform Retry    : 5
Probe Mode      : Disabled
Engine ID       :
Security Name   : None
STP                : Enabled
RMON               : Enabled

# show snmp host system
Trap Global Mode: disabled
Trap TestTrp-1 (ID:0) is disabled
Community       : public
Destination Host: 192.168.1.30
UDP Port        : 162
Version         : V3
Inform Mode     : Enabled
Inform Timeout  : 3
Inform Retry    : 5
Probe Mode      : Disabled
Engine ID       :
Security Name   : None
```

```
Warm Start         : Enabled
Cold Start         : Enabled

# show snmp host aaa
Trap Global Mode: disabled
# show snmp host aaa
Trap Global Mode: enabled
Trap trapOne (ID:0) is enabled
Community       : Public
Destination Host: 192.168.1.30
UDP Port        : 162
Version         : V2C
Inform Mode     : enabled
Inform Timeout  : 3
Inform Retry    : 5
Authentication Fail: enabled

#
```

Show SNMP Parameters Summary

show snmp
show snmp access [<group_name> { v1 | v2c | v3 | any } { auth | noauth | priv }]
show snmp community v3 [<community>]
show snmp host [<conf_name>] [system] [switch] [interface] [aaa]
show snmp mib context
show snmp mib ifmib ifIndex
show snmp security-to-group [{ v1 | v2c | v3 } <security_name>]
show snmp user [<username> <engineID>]
show snmp view [<view_name> <oid_subtree>]

Command: Show STP Bridge

Syntax:
show spanning-tree [summary | active | { interface (<port_type> [<v_port_type_list>]) } | { detailed [interface (<port_type> [<v_port_type_list_1>])] } | { mst [configuration | { <instance> [interface (<port_type> [<v_port_type_list_2>])] }] }]

Description: Display the current Spanning Tree data (active, detailed, interface, MST, and summary).
| : Output modifiers
active : STP active interfaces
detailed : STP statistics
interface : Choose port
mst : Configuration
summary : STP summary
<***cr***> : Show all.

Mode: #

Example: Display the current spanning tree config parameters:

```
# show spanning-tree ?
active     detailed   interface  mst        summary    |          <cr>
# show spanning-tree?
    spanning-tree    STP Bridge
    <cr>
# show spanning-tree
CIST Bridge STP Status
Bridge ID    : 32768.00-C0-F2-21-DB-83
Root ID      : 32768.00-C0-F2-21-DB-83
Root Port    : -
Root PathCost: 0
Regional Root: 32768.00-C0-F2-21-DB-83
Int. PathCost: 0
Max Hops     : 20
TC Flag      : Steady
TC Count     : 0
TC Last      : -
Port       Port Role       State       Pri  PathCost  Edge  P2P  Uptime
---------  --------------  ----------  ---  --------  ----  ---  -------------
# show spanning-tree active
CIST Bridge STP Status
Bridge ID    : 32768.00-C0-F2-21-DB-83
Root ID      : 32768.00-C0-F2-21-DB-83
Root Port    : -
Root PathCost: 0
Regional Root: 32768.00-C0-F2-21-DB-83
Int. PathCost: 0
Max Hops     : 20
TC Flag      : Steady
TC Count     : 0
TC Last      : -
Port       Port Role       State       Pri  PathCost  Edge  P2P  Uptime
---------  --------------  ----------  ---  --------  ----  ---  -------------
# show spanning-tree detailed
Port       Rx MSTP   Tx MSTP   Rx RSTP   Tx RSTP   Rx STP   Tx STP   Rx TCN   Tx TCN   Rx Ill.  Rx Unk.
---------  --------  --------  --------  --------  -------  -------  -------  -------  -------  -------
# show spanning-tree interface ?
    *                    All switches or All ports
    ManagementPort       Management Port
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
```

```
# show spanning-tree interface *
Mst    Port       Port Role       State       Pri  PathCost  Edge  P2P  Uptime
-----  ---------  --------------  ----------  ---  --------  ----  ---  --------
# show spanning-tree mst
CIST Bridge STP Status
Bridge ID    : 32768.00-C0-F2-21-DB-83
Root ID      : 32768.00-C0-F2-21-DB-83
Root Port    : -
Root PathCost: 0
Regional Root: 32768.00-C0-F2-21-DB-83
Int. PathCost: 0
Max Hops     : 20
TC Flag      : Steady
TC Count     : 0
TC Last      : -
Mst    Port       Port Role       State       Pri  PathCost  Edge  P2P  Uptime
-----  ---------  --------------  ----------  ---  --------  ----  ---  -------------
# show spanning-tree mst config
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
# show spanning-tree summary ?
    |       Output modifiers
    <cr>

# show spanning-tree summary
Protocol Version: MSTP
Max Age         : 20
Forward Delay   : 15
Tx Hold Count   : 6
Max Hop Count   : 20
BPDU Filtering  : Disabled
BPDU Guard      : Disabled
Error Recovery  : Disabled
CIST Bridge is active
#
```

The S4224 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 S4224 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 S4224 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 S4224 also supports configuration options for enabling/disabling BPDU guard, path cost for that port, restricting topology change notification, etc.

Command: Show Switching Mode Characteristics

Syntax: **show switchport forbidden** [{ vlan <vid> } | { name <name> }]
Description: Display the current switching mode characteristics.
Mode: #
Example:

```
# show switchport ?
    forbidden    Lookup VLAN Forbidden port entry.
# show switchport?
show switchport forbidden [ { vlan <vlan_id> } | { name <word> } ]
# show switchport forbidden ?
    |       Output modifiers
    name    name - Show forbidden access for specific VLAN name.
    vlan    vid - Show forbidden access for specific VLAN id.
    <cr>
# show switchport forbidden | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show switchport forbidden name
% Incomplete command.

# show switchport forbidden name ?
    <word>    VLAN name
# show switchport forbidden vlan ?
    <vlan_id>    VLAN id
# show switchport forbidden vlan 1
Forbidden VLAN table is empty for VLAN ID 1
#
```

Command: Show System CPU Status

Syntax: **show system cpu status**
Description: Display the current system CPU status.
Mode: #
Example:

```
# show system?
show system cpu status
# show system cpu status ?
    |       Output modifiers
    <cr>
# show system cpu status
    Average load in 100 ms  : 0%
    Average load in   1 sec : 6%
    Average load in  10 sec : 8%
# show system cpu status | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show system cpu status |
```

Command: Show TACACS+ Config

Syntax: **show tacacs-server**
Description: Display the current TACACS+ configuration.
Mode: #
Example:

```
# show tacacs-server
Global TACACS+ Server Timeout      : 9 seconds
Global TACACS+ Server Deadtime     : 1 minutes
Global TACACS+ Server Key          : mASTER
TACACS+ Server #1:
  Host name  : MasterSrvr1
  Port       : 49
  Timeout    : 9 seconds
  Key        : mASTER
#
# show tacacs-server?
    tacacs-server    TACACS+ configuration
    <cr>
# show tacacs-server ?
    |       Output modifiers
    <cr>
# show tacacs-server | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show tacacs-server |
```

Messages: *No hosts configured!*
No servers configured!

Command: Show Terminal Config

Syntax: **show terminal**

Description: Display the current terminal configuration parameters.

Mode: #

Example:

```
# show term
Line is con 0.
    * You are at this line now.
    Alive from Console.
    Default privileged level is 2.
    Command line editing is enabled
    Display EXEC banner is enabled.
    Display Day banner is enabled.
    Terminal width is 80.
             length is 24.
             history size is 32.
             exec-timeout is 10 min 0 second.

    Current session privilege is 15.
    Elapsed time is 0 day 0 hour 20 min 38 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

# show terminal ?
    |       Output modifiers
    <cr>
# show terminal | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
#
```

Command: Show UDLD

Syntax: **show udld** [interface (<port_type> [<plist>])]

Description: Display UDLD (Uni Directional Link Detection) configurations, statistics and status. The UDLD protocol monitors the physical configuration of the links between devices and ports that support UDLD. It detects the existence of unidirectional links.Its functionality is to provide mechanisms useful for detecting one way connections before they create a loop or other protocol malfunction. RFC 5171 specifies a way at the data link layer to detect Uni directional link.

Mode: #

Example 1: Display the current udld interface config:

```
# show udld ?
    |            Output modifiers
    interface    Choose port
    <cr>
# show udld interface ?
    *                    All switches or All ports
    ManagementPort       Management Port
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
# show udld interface GigabitEthernet ?
    <port_type_list>    Port list in 1/1-4
# show udld interface GigabitEthernet 1/1-2

GigabitEthernet 1/1
---------------------------------------------------------------------
UDLD Mode                 : Normal
Admin State               : Enable
Message Time Interval(Sec): 10
Device ID(local)          : 00-C0-F2-56-1A-90
Device Name(local)        :
Bidirectional state       : Indeterminant

No neighbor cache information stored
--------------------

GigabitEthernet 1/2
---------------------------------------------------------------------
UDLD Mode                 : Normal
Admin State               : Enable
Message Time Interval(Sec): 10
Device ID(local)          : 00-C0-F2-56-1A-90
Device Name(local)        :
Bidirectional state       : Indeterminant

No neighbor cache information stored
--------------------
#
```

Command: Show User Privilege Configuration

Syntax: **show user-privilege**

Description: Display Users privilege configuration.

Mode: #

Example 1: Display Users privilege configuration, configure, and then redisplay:

```
# show user-privilege ?
    <cr>
# show user-privilege
username admin privilege 15 password none
# show user-privilege?
    user-privilege    Users privilege configuration
    <cr>
# show user-privilege ?
    <cr>
# show user-privilege
username admin privilege 15 password none
(config)# username ?
    <word31>    User name allows letters, numbers and underscores
(config)# username Bob ?
    privilege    Set user privilege level
(config)# username Bob privilege ?
    <0-15>    User privilege level
(config)# username Bob privilege 10 ?
    password    Specify the password for the user
(config)# username Bob privilege 10 password ?
    encrypted      Specifies an ENCRYPTED password will follow
    none           NULL password
    unencrypted    Specifies an UNENCRYPTED password will follow
(config)# username Bob privilege 10 password unencrypted semaphore
(config)# end
# show user-privilege
username Bob privilege 10 password encrypted c2VtYXBob3Jl
username admin privilege 15 password none
#
```

Command: Show Users' Info

Syntax: **show users**
Description: Display the current user info (User name, Priv level, Elapsed time, and Idle time).
Mode: #
Example:

```
# show users ?
    |         Output modifiers
    myself    Display information about mine
    <cr>
# show users?
    users    Display information about terminal lines
    <cr>
# show users
Line is con 0.
    * You are at this line now.
    Connection is from Console.
    User name is admin.
    Privilege is 15.
    Elapsed time is 0 day 0 hour 22 min 57 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

# show users | ?
    begin      Begin with the line that matches
    exclude    Exclude lines that match
    include    Include lines that match
# show users myself ?
    |       Output modifiers
    <cr>
# show users myself
Line is con 0.
    * You are at this line now.
    Connection is from Console.
    User name is admin.
    Privilege is 15.
    Elapsed time is 0 day 0 hour 23 min 28 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

#
```

Command: Show Version Info

Syntax: **show version** [brief]

Description: Display the current System hardware build and software status.

Mode: #

Example: Display the show version options and output.

```
# show ver brief
Version      : S4224 (standalone) 2.2.1
Build Date   : 2015-07-15T17:19:44-05:00
# show ver

MEMORY           : Total=73562 KBytes, Free=42940 KBytes, Max=41957 KBytes
FLASH            : 0x40000000-0x40ffffff, 256 x 0x10000 blocks
MAC Address      : 00-c0-f2-56-16-d0
Previous Restart : Cool

Software ID     : S4224
Product ID      : S4224
Serial #        : 3012
Board Rev       : 3
FPGA Version    : v2.3
Board Temp      : 36 C
CPU Temp        : 45 C

System Contact   :
System Name      :
System Location  :
System Time      : 1970-01-01T00:01:48+00:00
System Uptime    : 00:01:48

Active Image
------------
-- more --, next page: Space, continue: g, quit: ^C
```

Command: Show VLAN Information

Syntax: **show vlan**

show vlan [id <vlan_list> | name <name> | brief] [all]
show vlan ip-subnet [<ipv4>]
show vlan mac [address <mac_addr>]
show vlan protocol [eth2 { <etype> | arp | ip | ipx | at }] [snap { <oui> | rfc-1042 | snap-8021h } <pid>] [llc <dsap> <ssap>]
show vlan status [interface (<port_type> [<plist>])] [admin | all | combined | conflicts | erps | evc | gvrp | mep | mstp | mvr | nas | rmirror | vcl | voice-vlan]

Description: Display the current VLAN status. VLAN (Virtual LAN) is a method used to restrict communication between S4224 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 S4224 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.

Mode: #

Example 1: Show the various **show vlan** sub-commands.

```
# show vlan?
    vlan    VLAN status
    <cr>
# show vlan <Tab>
all         brief      id         ip-subnet  mac        name       protocol
status      <cr>
# show vlan ?
    all          Show all VLANs (If left out only static VLANs are shown)
    brief        VLAN summary information
    id           VLAN status by VLAN id
    ip-subnet    Show VCL IP Subnet entries.
    mac          Show VLAN MAC entries.
    name         VLAN status by VLAN name
    protocol     Protocol-based VLAN status
    status       Show the VLANs configured for each interface.
    <cr>
# show vlan all
VLAN  Name                            Interfaces
----  ------------------------------  ----------
1     default                         Mgmt 1/1 Gi 1/1-24 10G 1/1-4

# show vlan brief
VLAN  Name                            Interfaces
----  ------------------------------  ----------
1     default                         Mgmt 1/1 Gi 1/1-24 10G 1/1-4

#
```

Example 2: Show the **show vlan** sub-commands' parameters.

```
# show vlan id ?
    <vlan_list>    VLAN IDs 1-4095
# show vlan id 1-3
VLAN  Name                            Interfaces
----  ------------------------------  ----------
1     default                         Mgmt 1/1 Gi 1/1-24 10G 1/1-4
2     VLAN0002
3     VLAN0003

#
# show vlan ip-subnet ?
    <ipv4_subnet>    Specify a specific IP Subnet.
    <cr>
# show vlan ip-subnet id ?
    <1-128>    The specific ip-subnet to show.
# show vlan ip-subnet id 1
Entry with VCE ID 1 not found
# show vlan mac ?
    address    Show a specific MAC entry.
    <cr>
# show vlan mac address ?
    <mac_ucast>    The specific MAC entry to show.
# show vlan mac address 00-00-00-00-00-01
Entry with MAC address 00-00-00-00-00-01 was not found in the switch/stack
# show vlan name ?
    <vword32>    A VLAN name
# show vlan protocol ?
    eth2    Ethernet protocol based VLAN status
    llc     LLC-based VLAN status
    snap    SNAP-based VLAN status
    <cr>
# show vlan protocol eth2 ?
    <0x600-0xffff>    Ether Type(Range: 0x600 - 0xFFFF)
    arp               Ether Type is ARP
    at                Ether Type is AppleTalk
    ip                Ether Type is IP
    ipx               Ether Type is IPX

# show vlan protocol eth2 ip
Entry not found
# show vlan status ?
    admin        Show the VLANs configured by administrator.
    all          Show all VLANs configured.
    combined     Show the VLANs configured by a combination.
    conflicts    Show VLANs configurations that has conflicts.
    erps         Show the VLANs configured by ERPS.
    evc          Show the VLANs configured by EVC.
    gvrp         Show the VLANs configured by GVRP.
    interface    Show the VLANs configured for a specific interface(s).
    mep          Show the VLANs configured by MEP.
    mstp         Show the VLANs configured by MSTP.
    mvr          Show the VLANs configured by MVR.
    nas          Show the VLANs configured by NAS.
    rmirror      Show the VLANs configured by Remote mirroring.
    vcl          Show the VLANs configured by VCL.
    <cr>
```

Example 3: Show the show vlan status parameters.

```
# show vlan status all
GigabitEthernet 1/1 :
---------------------
VLAN User   PortType       PVID  Frame Type     Ing Filter  Tx Tag             UVID  Conflicts
----------  -------------  ----  -------------  ----------  -----------------  ----  ---------
Combined    C-Port         1     All            Enabled     None               1       No
Admin       C-Port         1     All            Enabled     None               1
NAS                                                                                    No
GVRP                                                                                   No
MVR                                                                                    No
MSTP                                                                                   No
ERPS                                                                                   No
MEP                                                                                    No
-- more --, next page: Space, continue: g, quit: ^C
```

Example 4: Show the show vlan status for **mep** and **rmirror** parameters.

```
# show vlan status mep
GigabitEthernet 1/1 :
---------------------
VLAN User   PortType       PVID  Frame Type     Ing Filter  Tx Tag             UVID  Conflicts
----------  -------------  ----  -------------  ----------  -----------------  ----  ---------
MEP                                                                                    No

GigabitEthernet 1/2 :
---------------------
VLAN User   PortType       PVID  Frame Type     Ing Filter  Tx Tag             UVID  Conflicts
----------  -------------  ----  -------------  ----------  -----------------  ----  ---------
MEP                                                                                    No

GigabitEthernet 1/3 :
---------------------
VLAN User   PortType       PVID  Frame Type     Ing Filter  Tx Tag             UVID  Conflicts
# show vlan status rmirror ?
    interface    Show the VLANs configured for a specific interface(s).
    <cr>
# show vlan status rmirror
GigabitEthernet 1/1 :
---------------------
VLAN User   PortType       PVID  Frame Type     Ing Filter  Tx Tag             UVID  Conflicts
----------  -------------  ----  -------------  ----------  -----------------  ----  ---------
Rmirror                                                                                No

GigabitEthernet 1/2 :
---------------------
VLAN User   PortType       PVID  Frame Type     Ing Filter  Tx Tag             UVID  Conflicts
----------  -------------  ----  -------------  ----------  -----------------  ----  ---------
Rmirror                                                                                No

GigabitEthernet 1/3 :
---------------------
VLAN User   PortType       PVID  Frame Type     Ing Filter  Tx Tag             UVID  Conflicts
-- more --, next page: Space, continue: g, quit: ^C
```

Message: *Entry with IP subnet x was not found in the switch/stack*
Meaning: You entered a command (e.g., **show vlan ip-subnet id 100**) that does not exist.
Recovery: Either create the VLAN or enter the VID of another VLAN.

Command: Show Web Privilege Levels

Syntax: **show web privilege group** [<group_name>] level
Description: Display the current web privilege command levels. A user cannot access or execute a command unless the logged in user has sufficient priveleges assigned. (Not to be confused with User Exec mode and Privileged EXEC mode priveleges.)
Mode: #
Example: Display the show web privilege sub-commands.

```
# show web privilege group ?
    <cword>    Valid words are 'Aggregation' 'DDMI' 'DHCP' 'DHCPv6_Client'
               'Debug' 'Diagnostics' 'EPS' 'ERPS' 'ETHER_SAT' 'ETH_LINK_OAM'
               'EVC' 'IP' 'IPMC_Snooping' 'LACP' 'LLDP' 'Loop_Protect'
               'MAC_Table' 'MEP' 'MVR' 'Maintenance' 'NTP' 'PTP'
               'Performance_Monitor' 'Ports' 'Private_VLANs' 'QoS' 'RMirror'
               'Security' 'Spanning_Tree' 'System' 'UDLD' 'VCL'
               'VLAN_Translation' 'VLANs' 'XXRP'
    level      Web privilege group level
# show web privilege group agg ?
    level    Web privilege group level
# show web privilege group agg level ?
    |       Output modifiers
    <cr>
# show web privilege group agg level
Group Name                       Privilege Level
                                 CRO CRW SRO SRW
-------------------------------- --- --- --- ---
Aggregation                        5  10   5  10
# show web privilege group dhcp level
Group Name                       Privilege Level
                                 CRO CRW SRO SRW
-------------------------------- --- --- --- ---
DHCP                               5  10   5  10
# show web privilege group ip level
Group Name                       Privilege Level
                                 CRO CRW SRO SRW
-------------------------------- --- --- --- ---
IP                                 5  10   5  10
# show web privilege group maint level
Group Name                       Privilege Level
                                 CRO CRW SRO SRW
-------------------------------- --- --- --- ---
Maintenance                       15  15  15  15
#
```

These commands let you display and configure the user privilege levels. The valid range is 1 - 15. If the privilege level 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. 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.

The user Privilege Level parameters are:

- <**cro**> : **C**onfiguration **r**ead-**o**nly privilege level (1-15).
- <**crw**> : **C**onfiguration/Execute **r**ead-**w**rite privilege level (1-15).
- <**sro**> : **S**tatus/Statistics **r**ead-**o**nly privilege level (1-15).
- <**srw**> : **S**tatus/Statistics **r**ead-**w**rite privilege level (1-15).

Terminal Commands

Command: Set Terminal Parameters

Syntax: **terminal**

Description: Set terminal line parameters, where:

terminal editing : Enable command line editing.
terminal exec-timeout : Set the EXEC timeout in minutes <0-1440> [<0-3600>].
terminal help : Description of the interactive help system.
terminal history size : Set the number of history commands stored; <0-32>;
0 = disable storing history.
terminal length : Set number of lines on a screen <0, 3-512>; (0 = no pausing).
terminal width : Set width of the display terminal <0, 40-512>; (0 = unlimited width).

Mode: #

Example:

```
# terminal ?
editing         Enable command line editing
exec-timeout    Set the EXEC timeout
help            Description of the interactive help system
history         Control the command history function
length          Set number of lines on a screen
width           Set width of the display terminal
# terminal exec-timeout ?
    <0-1440>    Timeout in minutes
# terminal help ?
    <cr>
# terminal help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)

# terminal history size ?
    <0-32>    Number of history commands, 0 means disable
# terminal length ?
    0 or 3-512    Number of lines on screen (0 for no pausing)
# terminal width ?
    0 or 40-512    Number of characters on a screen line (0 for unlimited
                   width)
# terminal width
```

Veriphy Commands

Command: Veriphy Interface

Syntax: **veriphy** [{ interface (<port_type> [<v_port_type_list>]) }]

Description: The VeriPHY commands are used for running the VeriPHY Cable Diagnostics. This will take approximately five seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length of 7 - 140 meters. The 10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete. The reported parameters are:

Interface : The interface for which you are requesting VeriPHY Cable Diagnostics.
Pair: : The status of the cable pair.
OK - Correctly terminated pair.
Open - Open pair.
Short : The Shorted pair.
Length : The length (in meters) of the cable pair. The resolution is 3 meters.

Mode: #

Example: Show the various VeriPhy commands and run a VeriPhy test.

```
# veriphy ?
    interface    Interface keyword
    <cr>
# veriphy interface ?
    *                    All switches or All ports
    ManagementPort       Management Port
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
# veriphy interface * ?
    <port_type_list>    Port list for all port types
    <cr>
# veriphy interface *
Starting VeriPHY - Please wait
Interface               Pair A  Length  Pair B, Length  Pair C  Length  Pair D  Length
----------------------  ------  ------  --------------  ------  ------  ------  -------
ManagementPort 1/1      Open    3       Short C 2       OK      49      OK      49
GigabitEthernet 1/1     No test results
GigabitEthernet 1/2     No test results
GigabitEthernet 1/3     No test results
GigabitEthernet 1/4     No test results
GigabitEthernet 1/5     No test results
```

S4224 Command / Parameters Summary

```
# ?
    clear        Reset functions
    configure    Enter configuration mode
    copy         Copy from source to destination
    delete       Delete one file in flash: file system
    dir          Directory of all files in flash: file system
    disable      Turn off privileged commands
    do           To run exec commands in config mode
    dot1x        IEEE Standard for port-based Network Access Control
    enable       Turn on privileged commands
    exit         Exit from EXEC mode
    firmware     Firmware upgrade/swap
    help         Description of the interactive help system
    ip           IPv4 commands
    ipv6         IPv6 configuration commands
    link-oam     Link OAM configuration
    logout       Exit from EXEC mode
    more         Display file
    no           Negate a command or set its defaults
    ping         Send ICMP echo messages
    ptp          Misc non persistent 1588 settings
    reload       Reload system.
    send         Send a message to other tty lines
    show         Show running system information
    terminal     Set terminal line parameters
    veriphy      Veriphy keyword
# ??
clear access management statistics
clear access-list ace statistics
clear dot1x statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]
clear eps <inst> wtr
clear erps [ <groups> ] statistics
clear evc statistics { [ <evc_id> | all ] } [ ece [ <ece_id> ] ] [ interface ( <port_type> [ <port_list> ]
) ] [ pw <pw_num_list> ]
clear ip arp
clear ip dhcp detailed statistics { server | client | snooping | relay | helper | all } [ interface (
<port_type> [ <in_port_list> ] ) ]
clear ip dhcp relay statistics
clear ip dhcp server binding <ip>
clear ip dhcp server binding { automatic | manual | expired }
clear ip dhcp server statistics
clear ip dhcp snooping statistics [ interface ( <port_type> [ <in_port_list> ] ) ]
clear ip igmp snooping [ vlan <v_vlan_list> ] statistics
clear ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]
clear ipv6 mld snooping [ vlan <v_vlan_list> ] statistics
clear ipv6 neighbors
clear ipv6 statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]
clear lacp statistics
clear link-oam statistics [ interface ( <port_type> [ <plist> ] ) ]
clear lldp statistics { [ interface ( <port_type> [ <plist> ] ) ] | global }
clear logging [ informational ] [ notice ] [ warning ] [ error ] [ switch <switch_list> ]
clear mac address-table
clear mep <inst> { lm | dm | tst | bfd }
clear mvr [ vlan <v_vlan_list> | name <mvr_name> ] statistics
clear network-clock clk-source <clk_list>
clear spanning-tree { { statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ] } | { detected-
protocols [ interface ( <port_type> [ <v_port_type_list_1> ] ) ] } }
clear statistics [ interface ] ( <port_type> [ <v_port_type_list> ] )
configure terminal
copy { startup-config | running-config | <source_path> } { startup-config | running-config |
<destination_path> } [ syntax-check ]
delete <path>
dir
disable [ <new_priv> ]
do <command>
dot1x initialize [ interface ( <port_type> [ <plist> ] ) ]
```

```
enable [ <new_priv> ]
exit
firmware swap
firmware upgrade <tftpserver_path_file> [ activate { now | defer } ]
help
ip dhcp retry interface vlan <vlan_id>
ipv6 dhcp-client restart [ interface vlan <v_vlan_list> ]
link-oam remote-loopback { start | stop } interface ( <port_type> [ <v_port_type_list> ] )
logout
more <path>
no debug interrupt-monitor source <source>
no debug ipv6 nd
no debug trace hunt
no port-security shutdown [ interface ( <port_type> [ <v_port_type_list> ] ) ]
no ptp <clockinst> wireless mode interface ( <port_type> [ <v_port_type_list> ])
no terminal editing
no terminal exec-timeout
no terminal history size
no terminal length
no terminal width
ping ip { <v_ip_addr> | <v_ip_name> } [ repeat <count> ] [ size <size> ] [ interval <seconds> ]
ping ipv6 { <v_ipv6_addr> | <v_ipv6_name> } [ repeat <count> ] [ size <size> ] [ interval <seconds> ] [
interface vlan <v_vlan_id> ]
ptp <clockinst> local-clock { update | ratio <ratio> }
ptp <clockinst> wireless delay <base_delay> [ <incr_delay> ] interface ( <port_type> [ <v_port_type_list>
] )
ptp <clockinst> wireless mode interface ( <port_type> [ <v_port_type_list> ] )
ptp <clockinst> wireless pre-notification interface ( <port_type> [ <v_port_type_list> ] )
reload { { { cold | warm } [ sid <usid> ] } | { defaults [ keep-ip ] } }
send { * | <session_list> | console 0 | vty <vty_list> } <message>
show aaa
show access management [ statistics | <access_id_list> ]
show access-list [ interface [ ( <port_type> [ <v_port_type_list> ] ) ] ] [ rate-limiter [
<rate_limiter_list> ] ] [ ace statistics [ <ace_list> ] ]
show access-list ace-status [ static ] [ link-oam ] [ loop-protect ] [ dhcp ] [
ptp ] [ upnp ] [ arp-inspection ] [ evc ] [ mep ] [ ipmc ] [ ip-source-guard ] [ ip-mgmt ] [ conflicts ] [
switch <switch_list> ]
show aggregation [ mode ]
show clock
show clock detail
show ddmi
show dot1x statistics { eapol | radius | all } [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show dot1x status [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ brief ]
show eps [ <inst> ] [ detail ]
show erps { [ <groups> ] } [ detail | statistics ]
show ethersat config
show ethersat loopback { config | state | testsideport | smac | vid | timeout }
show ethersat loopback { status }
show ethersat profile <pid> config
show ethersat profile <pid> frameformat
show evc statistics { [ <evc_id> | all ] } [ ece [ <ece_id> ] ] [ interface ( <port_type> [ <port_list> ]
) ] [ pw <pw_num_list> ] [ cos <cos> ] [ green | yellow | red | discard ] [ frames | bytes ]
show evc { [ <evc_id> | all ] } [ ece [ <ece_id> ] ]
show green-ethernet [ interface ( <port_type> [ <port_list> ] ) ]
show green-ethernet energy-detect [ interface ( <port_type> [ <port_list> ] ) ]
show green-ethernet short-reach [ interface ( <port_type> [ <port_list> ] ) ]
show history
show interface ( <port_type> [ <in_port_list> ] ) switchport [ access | trunk | hybrid ]
show interface ( <port_type> [ <plist> ] ) transceiver
show interface ( <port_type> [ <v_port_type_list> ] ) capabilities
show interface ( <port_type> [ <v_port_type_list> ] ) statistics [ { packets | bytes | errors | discards |
filtered | { priority [ <priority_v_0_to_7> ] } } ] [ { up | down } ]
show interface ( <port_type> [ <v_port_type_list> ] ) status
show interface ( <port_type> [ <v_port_type_list> ] ) veriphy
show interface vlan [ <vlist> ]
show ip arp
show ip arp inspection [ interface ( <port_type> [ <in_port_type_list> ] ) | vlan <in_vlan_list> ]
show ip arp inspection entry [ dhcp-snooping | static ] [ interface ( <port_type> [ <in_port_type_list> ]
) ]
```

```
show ip dhcp detailed statistics { server | client | snooping | relay | normal-forward | combined } [
interface ( <port_type> [ <in_port_list> ] ) ]
show ip dhcp excluded-address
show ip dhcp pool [ <pool_name> ]
show ip dhcp relay [ statistics ]
show ip dhcp server
show ip dhcp server binding <ip>
show ip dhcp server binding [ state { allocated | committed | expired } ] [ type { automatic | manual |
expired } ]
show ip dhcp server declined-ip
show ip dhcp server declined-ip <declined_ip>
show ip dhcp server statistics
show ip dhcp snooping [ interface ( <port_type> [ <in_port_list> ] ) ]
show ip dhcp snooping table
show ip domain
show ip http server secure status
show ip igmp snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [
<v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
show ip igmp snooping mrouter [ detail ]
show ip interface brief
show ip name-server
show ip route
show ip source binding [ dhcp-snooping | static ] [ interface ( <port_type> [ <in_port_type_list> ] ) ]
show ip ssh
show ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]
show ip verify source [ interface ( <port_type> [ <in_port_type_list> ] ) ]
show ipmc profile [ <profile_name> ] [ detail ]
show ipmc range [ <entry_name> ]
show ipv6 dhcp-client [ interface vlan <v_vlan_list> ]
show ipv6 interface [ vlan <v_vlan_list> { brief | statistics } ]
show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [
<v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
show ipv6 mld snooping mrouter [ detail ]
show ipv6 neighbor [ interface vlan <v_vlan_list> ]
show ipv6 route [ interface vlan <v_vlan_list> ]
show ipv6 statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]
show lacp { internal | statistics | system-id | neighbor }
show line [ alive ]
show link-oam { [ status ] [ link-monitor ] [ statistics ] } [ interface ( <port_type> [ <plist> ] ) ]
show lldp med media-vlan-policy [ <v_0_to_31> ]
show lldp med remote-device [ interface ( <port_type> [ <port_list> ] ) ]
show lldp neighbors [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show lldp statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show logging <log_id> [ switch <switch_list> ]
show logging [ informational ] [ notice ] [ warning ] [ error ] [ switch <switch_list> ]
show loop-protect [ interface ( <port_type> [ <plist> ] ) ]
show mac address-table [ conf | static | aging-time | { { learning | count } [ interface ( <port_type> [
<v_port_type_list> ] ) | vlan <v_vlan_id_2> ] } | { address <v_mac_addr> [ vlan <v_vlan_id> ] } | vlan
<v_vlan_id_1> | interface ( <port_type> [ <v_port_type_list_1> ] ) ]
show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck | pm | syslog | tlv |
bfd | rt | lst ] [ detail ]
show monitor [ session { <session_number> | all | remote } ]
show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [
<v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
show network-clock
show network-clock clock-selection-config
show network-clock source-nomination-config
show network-clock station-clock-config
show network-clock synchronization
show ntp status
show platform phy [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show platform phy id [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show platform phy instance
show platform phy mode [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show port-security switch [ interface ( <port_type> [ <v_port_type_list> ] ) ]
show privilege
show process list [ detail ]
show process load
```

```
show ptp <clockinst> local-clock
show ptp <clockinst> slave-cfg
show ptp <clockinst> slave-table-unicast
show ptp <clockinst> { default | current | parent | time-property | filter | servo | clk | ho | uni |
master-table-unicast | slave | { { port-state | port-ds | wireless | foreign-master-record } [ interface (
<port_type> [ <v_port_type_list> ] ) ] } }
show ptp ext-clock
show ptp system-time
show pvlan [ <pvlan_list> ]
show pvlan isolation [ interface ( <port_type> [ <plist> ] ) ]
show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-
translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
show radius-server [ statistics ]
show rmon alarm [ <id_list> ]
show rmon event [ <id_list> ]
show rmon history [ <id_list> ]
show rmon statistics [ <id_list> ]
show running-config [ all-defaults ]
show running-config feature <feature_name> [ all-defaults ]
show running-config interface ( <port_type> [ <list> ] ) [ all-defaults ]
show running-config interface vlan <list> [ all-defaults ]
show running-config line { console | vty } <list> [ all-defaults ]
show running-config vlan <list> [ all-defaults ]
show snmp
show snmp access [ <group_name> { v1 | v2c | v3 | any } { auth | noauth | priv } ]
show snmp community v3 [ <community> ]
show snmp host [ <conf_name> ] [ system ] [ switch ] [ interface ] [ aaa ]
show snmp mib context
show snmp mib ifmib ifIndex
show snmp security-to-group [ { v1 | v2c | v3 } <security_name> ]
show snmp user [ <username> <engineID> ]
show snmp view [ <view_name> <oid_subtree> ]
show spanning-tree [ summary | active | { interface ( <port_type> [ <v_port_type_list> ] ) } | { detailed
[ interface ( <port_type> [ <v_port_type_list_1> ] ) ] } | { mst [ configuration | { <instance> [
interface ( <port_type> [ <v_port_type_list_2> ] ) ] } ] } ]
show switchport forbidden [ { vlan <vid> } | { name <name> } ]
show system cpu status
show tacacs-server
show terminal
show udld [ interface ( <port_type> [ <plist> ] ) ]
show user-privilege
show users [ myself ]
show version [ brief ]
show vlan [ id <vlan_list> | name <name> | brief ] [ all ]
show vlan ip-subnet [ <ipv4> ]
show vlan mac [ address <mac_addr> ]
show vlan protocol [ eth2 { <etype> | arp | ip | ipx | at } ] [ snap { <oui> | rfc-1042 | snap-8021h }
<pid> ] [ llc <dsap> <ssap> ]
show vlan status [ interface ( <port_type> [ <plist> ] ) ] [ admin | all | combined | conflicts | erps |
evc | gvrp | mep | mstp | mvr | nas | rmirror | vcl | voice-vlan ]
show web privilege group [ <group_name> ] level
terminal editing
terminal exec-timeout <min> [ <sec> ]
terminal help
terminal history size <history_size>
terminal length <lines>
terminal width <width>
veriphy [ { interface ( <port_type> [ <v_port_type_list> ] ) } ]
##
```

11 Messages

Message:

% Error in file startup-config, line x:

% Invalid word detected at '^' marker.

% 1 problem found during configuration.

Example:

```
PW qos 00:00:01 30/tn_qos_port_conf_read#2563: Warning: isid:2, conf_sec_open()
failed or size mismatch, creating defaults
press ENTER to get startedW ether_sat 00:00:01 30/SA_conf_read_stack#289: Warning
: conf_sec_open failed or size mismatch, creating defaults
W ether_sat 00:00:01 30/SA_conf_read_stack#319: Warning: conf_sec_open failed or
 size mismatch, creating defaults
W ether_sat 00:00:01 30/SA_conf_read_stack#352: Warning: conf_sec_open failed or
 size mismatch, creating defaults
% Error in file startup-config, line 7:
aggregation mode
^
% Invalid word detected at '^' marker.

% 1 problem found during configuration.
```

Meaning: A reboot or similar function returned a config problem.

Recovery: 1. Verify the entry / operation. 2. Retry the operation; see the related section of this manual. 2. Reboot the device. 3. Upgrade the device firmware; see the ***firmware*** command. 4. Contact TN Technical Support.

Service, Warranty & Compliance Information

See the *S4224 Install Guide* manual for:

- Service
- Warranty
- Compliance Information
- Declaration of Conformity
- Electrical Safety Warnings
- Safety Instructions for Rack Mount Installations
- other related information

Contact Us

Technical Support

Technical support is available 24 hours a day.
US and Canada: 1-800-260-1312
International: 00-1-952-941-7600
Transition Now 7:00 AM to 6:00 PM CST
Voice Mail: 800-260-1312 x 579 or 952-941-7600 x 579
Chat live via the Web with Transition Networks Technical Support.
Log onto www.transition.com and click the Tech Support/Transition Now link.

Web-Based Seminars

Transition Networks provides seminars via live web-based training.
Log onto www.transition.com and click the Learning Center link.

E-Mail

To ask a question anytime, send an e-mail to our technical support staff at techsupport@transition.com.

Address

Transition Networks
10900 Red Circle Drive,
Minnetonka, MN 55343, U.S.A.
Telephone: 952-941-7600
Toll free: 800-526-9267
Fax: 952-941-2322

Related Manuals and Online Help

This manual is one of several S4224 manuals which include:

- S4224 Install Guide, 33557
- S4224 Quick Start Guide, 33636 (printed)
- S4224 User Guide, 33558
- S4224 CLI Reference, 33559 (this manual)
- Converge™ EMS Windows Install Guide (33543), Linux Install Guide (33533), Admin Procedures (33544)
- Release Notes (version specific)

For Product Information, Application Notes, etc., check the S4224 landing page at
http://www.transition.com/TransitionNetworks/Landing/S4224/S4224.aspx

Glossary

This section describes many of the terms and mnemonics used in this manual. Note that the use of or description of a term does not in any way imply support of that feature or of any related function(s).

1+1

The Protection Type 1+1 uses the protection resources at all times for sending a replica of the traffic. The protection merge point, where both copies are expected to arrive, decides which of the two copies to select for forwarding.
The decision can be to switch from one resource to the other due to an event like resource up/down etc. or can be on a per frame/cell basis, the selection decision is performed according to parameters defined below (e.g. revertive, non-revertive, manual, etc.).
A network can offer protection by providing alternative resources to be used when the working resource fails.
The specific terminology for the number and arrangement of such resources includes 1+1, 1:1, 1:n, n:1, and m:n.

1:1

The 1:1 Protection Type provides a protection resource for a single working resource.
A network can offer protection by providing alternative resources to be used when the working resource fails.
The terminology for the number and arrangement of such resources includes 1+1, 1:1, 1:n, n:1, and m:n.

1 PPS

In IEEE 1588v2, a pulse that is repeated every second and has a very accurate phase. It synchronizes several geographically dispersed clients (e.g., cell cites) to the same time and phase of 1 µs. Any third party test equipment must also support 1 PPS.

A

AAA

(Authentication, Authorization and Accounting); examples of this type of protocols include RADIUS, TACACS, TACACS+, etc. See the IETF Working Group status page (http://tools.ietf.org/wg/aaa/) for more information. For IETF RFC information see http://tools.ietf.org/html/rfc2975.

Authentication: refers to the process where an entity's identity is authenticated, typically by providing evidence that it holds a specific digital identity such as an identifier and the corresponding credentials. Examples of types of credentials are passwords, one-time tokens, digital certificates, and phone numbers (calling/called).

Authorization: determines whether a particular entity is authorized to perform a given activity, typically inherited from authentication when logging on to an application or service. Authorization may be determined based on a range of restrictions, for example time-of-day restrictions, or physical location restrictions, or restrictions against multiple access by the same entity or user. Typical authorization in everyday computer life is for example granting read access to a specific file for authenticated user. Examples of types of service include IP address filtering, address assignment, route assignment, quality of Service/differential services, bandwidth control/traffic management, compulsory tunneling to a specific endpoint, and encryption.

Accounting: refers to the tracking of network resource consumption by users for the purpose of capacity and trend analysis, cost allocation, billing.[3] In addition, it may record events such as authentication and authorization failures, and include auditing functionality, which permits verifying the correctness of procedures carried out based on accounting data. Real-time accounting refers to accounting information that is delivered concurrently with the consumption of

the resources. Batch accounting refers to accounting information that is saved until it is delivered at a later time. Typical information gathered includes the identity of the user or other entity, the nature of the service delivered, when the service began, when it ended, and if there is a status to report.

ACE

ACE (**A**ccess **C**ontrol **E**ntry) describes the access permission 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, different parameter options that are available for individual application.

ACE

(Associated Channel Header) IETF RFC 4835 specifies how the PW control word is used to distinguish a PW payload from an IP payload carried over an MPLS PSN. It then describes the preferred design of a PW Control Word to be useover an MPLS PSN, and the Pseudowire Associated Channel Header.

ACL

ACL is an acronym for **A**ccess **C**ontrol **L**ist. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights. ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.
There are three S4224 web pages associated with the manual ACL configuration:
`ACL|Access Control List`: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.
`ACL|Ports`: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property.
`ACL|Rate Limiters`: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

ActiPHY™

An automatic power savings mode when a specific port is in link down or standby operation. Actiphy® is a registered trademark used for Semiconductors, Integrated Circuits and Ethernet Transceivers and owned by Vitesse Semiconductor Corporation.

Address

Digital information that uniquely identifies a network, station, device, etc. so that each can send and receive messages. There are four types of addresses commonly used with the Internet:

- Email address (e.g., *name@mail_server.domain*)
- IP address or Internet address: *a.b.c.d* or *device_name.sub-domain.domain*
- MAC address (hardware address)
- URL (Uniform Resource Locator): *method://server_adress[port]/document_path*

Address

In IPv6, an IPv6-layer identifier for an interface or a set of interfaces.

Alarm

The term ‘alarm’ actually refers to all types of fault events that are associated with a potential failure. Per MEF 15, the Perceived Alarm Severity (critical, major, minor, warning, indeterminate, or cleared). Severity assignments are only required for equipment alarms and physical layer communications alarms generated by the ME-NE).
a. Critical - Indicates that a service affecting condition has occurred and immediate corrective action is required. Such a severity is used when the managed entity is totally out of service and its capability must be restored.
b. Major - Indicates that a service affecting condition has occurred and urgent corrective action is required. Such a severity is used when there is a severe degradation in the capability of the managed entity and its full capability must be restored.
c. Minor - Indicates that a non-service affecting condition has occurred and that corrective action should be taken in order to prevent a more serious fault.
d. Warning - Indicates the detection of a potential or impending service affecting fault, before any significant effects have been felt.
e. Indeterminate - The severity level cannot be determined.
f. Cleared - The clearing of one or more previously reported alarms.

Anycast address

In IPv6, an identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the "nearest" one, according to the routing protocol's measure of distance).

AES

AES is an acronym for **A**dvanced **E**ncryption **S**tandard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

AP

Access Point, such as a wireless Access Point defined by IEEE 802.11.

APS

APS is an acronym for **A**utomatic **P**rotection **S**witching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

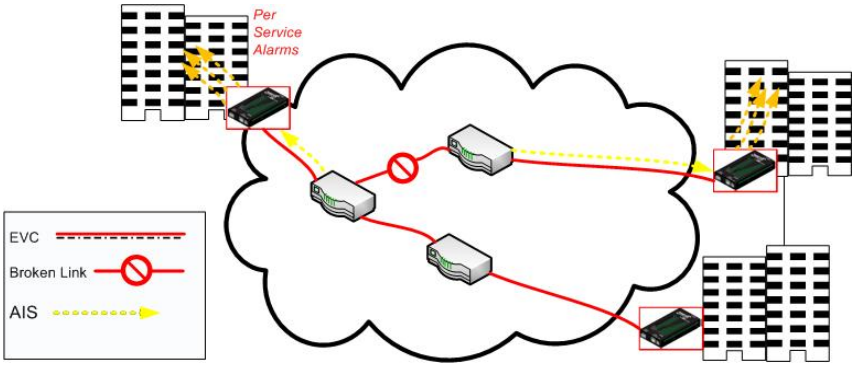
Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability. (Also *Port* Aggregation*, Link Aggregation*).

Alarm Indication Signal (AIS)

ETH-AIS allows alarm suppression when defects are to be detected at the server layer. You can enable or disable frames transmission with ETH-AIS information on an MEP or on a server MEP. You can also issue frames with ETH-AIS information at the client maintenance level by a MEP, including a server MEP, on detecting defect conditions. Defect conditions can include signal fail conditions with ETH-CC enabled, and AIS condition with ETH-CC disabled.

Only a MEP or Server MEP is configured to issue frames with ETH-AIS information. When a MEP detects a defect condition, it immediately starts transmitting periodic frames with ETH-AIS information at a configured client maintenance level. The MEP continues to transmit periodic frames with ETH-AIS information until the defect condition is resolved. On receiving a frame with ETH-AIS information, a MEP detects the AIS condition and suppresses loss of continuity alarms with all of its peer MEPs. The MEP resumes loss of continuity alarm generation on detecting loss of continuity conditions in place of the AIS condition.



Transmission of frames with ETH-AIS information can be enabled or disabled on a MEP (or on a server MEP). Frames with ETH-AIS information can be issued at the client MEG level by a MEP, including a server MEP, upon detecting defect conditions.

ARP

ARP is an acronym for **A**ddress **R**esolution **P**rotocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Automatic Reversion

The protection is in revertive mode if, after a resource failure and its subsequent repair, the network automatically reverts to using this initial resource. The protection is in non-revertive mode otherwise. Automatic reversion may include a reversion timer (i.e., the Wait To Restore), which delays the time of reversion after the repair.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

B

Bandwidth Profile

A characterization of ingress Service Frame arrival times and lengths at a reference point and a specification of the disposition of each Service Frame based on its level of compliance with the Bandwidth Profile. In MEF documents, the reference point is the UNI. See MEF 6.1.

BFD

Bidirectional Forwarding Detection (BFD) is a protocol intended to detect faults in the bidirectional path between two forwarding engines, including interfaces, data link(s), and to the extent possible the forwarding engines themselves, with potentially very low latency. BFD operates independently of media, data protocols, and routing protocols.See IETF RFC 5880 (https://tools.ietf.org/html/rfc5880) and 5881 (https://tools.ietf.org/html/rfc5881). IETF RFC 6428 specifies specific extensions to BFD and methods for proactive Continuity Check, Continuity Verification, and Remote Defect Indication for MPLS-TP pseudowires, Label Switched Paths, and Sections. See https://tools.ietf.org/html/rfc6428,

Boundary clock

A clock that has multiple Precision Time Protocol (PTP) ports in a domain and maintains the timescale used in the domain. It may serve as the source of time (i.e., be a master clock) and may synchronize to another clock (i.e., be a slave clock).
A Boundary Clock (BC) is a clock with more than a single PTP port, with each PTP port providing access to a separate PTP communication path. Boundary clocks are used to eliminate fluctuations produced by routers and similar network elements.

BPDU

Bridge Protocol Data Units are data messages that are exchanged across the switches within an extended LAN that uses a spanning tree protocol topology. BPDU packets contain information on ports, addresses, priorities and costs and ensure that the data ends up where it was intended to go. BPDU messages are exchanged across bridges to detect loops in a networktopology. The loops are then removed by shutting down selected bridge interfaces and placing redundant switch ports in a backup, or blocked, state.

Broadcast

A message forwarded to all (multiple, unspecified recipients) network destinations. On Ethernet, a broadcast packet is a special type of multicast packet where all nodes on the network are always willing to receive.

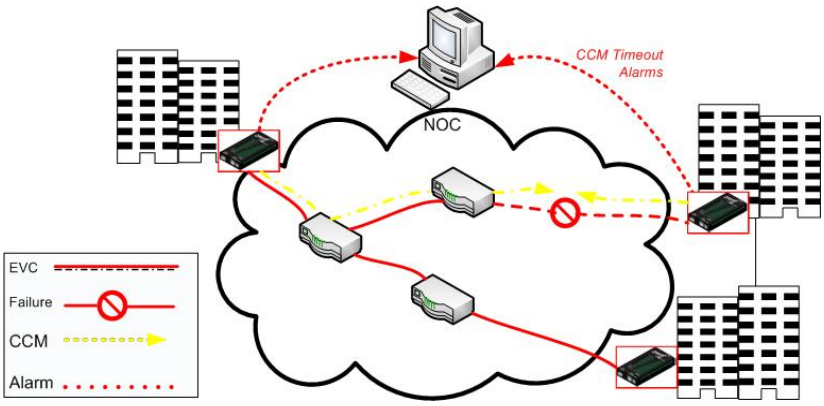
C

CC

CC (Continuity Check) is a MEP function that detects loss of continuity in a network by transmitting CCM frames to a peer MEP.

CC Monitoring (Continuity Checks Monitoring)

Fault detection uses the Continuity Check protocol to detect both connectivity failures and unintended connectivity between service instances. Each MEP can periodically transmit a multicast Connectivity Check Message (CCM) announcing the identity of the MEP and its MA, and tracks the CCMs received from the other MEPs. All connectivity faults that can misdirect a CCM show up as differences between the CCMs received and the MEP's configured expectations. The state of the tracked CCMs can be displayed.



Each Continuity Check Message (CCM) is a multicast CFM PDU transmitted periodically by a MEP to ensure continuity over the MA to which the transmitting MEP belongs. No reply is sent by any MP in response to receiving a CCM. CCMs use addresses from the Continuity Check Message Group Destination MAC Address table. The CCM can be sent away from or towards the MAC Relay Entity.

CCM

CCM is an acronym for **C**ontinuity **C**heck **M**essage. It is a OAM frame transmitted from a MEP to its peer MEP and used to implement CC functionality.

CDP

CDP (Cisco Discovery Protocol) is a Cisco proprietary Layer 2 protocol that is media- and protocol-independent, and runs on Cisco routers, bridges, access servers, and switches. A Cisco device with CDP enabled sends out periodic interface updates to a multicast address in order to make itself known to neighbors. As a layer two protocol, these packets (frames) are not routed. Using SNMP with the CDP MIB lets network management applications learn the device type and the SNMP agent address of neighboring devices, and to then send SNMP queries to those devices.

CIST

Acronym for **C**ommon and **I**nternal **S**panning **T**ree. Concerning IST/CST/CIST, IST is the only instance that can send and receive BPDUs in the MST network. An MSTn instance is local to a region. ISTs in different regions are interconnected via a Common Spanning Tree (CST). The CIST includes the collection of ISTs in each MST region, and the CST that connects the ISTs.
The CIST is the default spanning tree instance of MSTP (i.e., all VLANs that are not members of particular MSTIs are members of the CIST. Also, an individual MST region can be regarded a single virtual bridge by other MST regions. The spanning tree that runs between MSTP regions is the CIST.

Clock

In PTP, a node participating in the Precision Time Protocol (PTP) that is capable of providing a measurement of the passage of time since a defined epoch.

Commonly Used EtherTypes

The 'EtherType' field in an Ethernet frame indicates the protocol used in the data field of the frame. According to the IEEE 802.3, Length/EtherType field is a two-octet field which takes one of two meanings, depending on its numeric value. For numeric evaluation, the first octet is the most significant octet; when the value of this field is ≥ 1536 decimal (0600 hex) the EtherType field indicates the nature of the MAC client protocol (EtherType interpretation). The value of the Type Field is obtained from the IEEE EtherType Field Registrar. The EtherType field is a very limited space and assignments are limited. The EtherType field is administered by the IEEE RAC EtherType Field Approval Authority. The following list of EtherTypes is unverified information from various sources.

EtherType (hex)	Protocol
0x000 - 0x05DC	IEEE 802.3 length
0x0101-0x01FF	Experimental
0x0600	Xerox NS IDP
0x0660, 0x0661	DLOG
0x0800	IP (Internet Protocol)
0x0801	X.75 Internet
0x0802	NBS Internet
0x0803	ECMA Internet
0x0804	Chaosnet
0x0805	X.25 Level 3
0x0806	ARP (Address Resolution Protocol)
0x0808	Frame Relay ARP (RFC 1701)
0x6559	Raw Frame Relay (RFC 1701)
0x8035	RARP (Reverse Address Resolution Protocol), DRAP (Dynamic RARP)
0x80F3	AARP, AppleTalk Address Resolution Protocol
0x8100	VLAN-tagged frame (IEEE 802.1Q)
0x8137	IPX (Internet Packet Exchange)
0x814c	SNMP (Simple Network Management Protocol)
0x86DD	IPv6 (Internet Protocol version 6)
0x8808	MAC Control
0x8809	Slow Protocols (IEEE 802.3)
0x880B	PPP (Point to Point Protocol)
0x880C	GSMP (General Switch Management Protocol)
0x8819	CobraNet

0x8847	MPLS (Multi-Protocol Label Switching) (unicast)
0x8848	MPLS (Multi-Protocol Label Switching) (multicast)
0x8863	PPoE (PPP over Ethernet) (Discovery stage)
0x8864	PPoE (PPP over Ethernet) (PPP Session stage)
0x886F	Microsoft NLB heartbeat
0x8870	Jumbo Frames
0x887B	HomePlug 1.0 MME
0x888E	EAPOL (EAP over LAN) (IEEE 802.1X)
0x88BB	LWAP (Light Weight Access Point Protocol)
0x88CC	LLDP (Link Layer Discovery Protocol)
0x8892	PROFINET Protocol
0x889A	HyperSCSI (SCSI over Ethernet)
0x88A2	ATA over Ethernet
0x88A4	EtherCAT Protocol
0x88A8	Provider Bridging (IEEE 802.1ad)
0x88AB	Ethernet Powerlink
0x88CC	LLDP
0x88CD	SERCOS III
0x88D8	Circuit Emulation Services over Ethernet (MEF-8)
0x88E1	HomePlug AV MME
0x88E5	MAC security (IEEE 802.1AE)
0x88F7	Precision Time Protocol (IEEE 1588)
0x8902	IEEE 802.1ag Connectivity Fault Management (CFM) Protocol / ITU-T Recommendation Y.1731 (OAM)
0x8906	Fibre Channel over Ethernet
0x8914	FCoE Initialization Protocol
0x9000	Loopback (Configuration test protocol)
0x9100	VLAN Tag Protocol Identifier (Q-in-Q)
0x9200	VLAN Tag Protocol Identifier
0xCAFE	Veritas LLT (Low Latency Transport)
0xFFFF	(Reserved)

Note: Some well known EtherTypes are not necessarily listed in the IEEE list of EtherType values. For example, EtherType 0x0806 (used by ARP) is listed by the IEEE only as "Symbolics, Inc., Protocol unavailable."
See http://standards.ieee.org/develop/regauth/ethertype/eth.txt for more information.

The EtherType is one of two types of protocol identifier parameters that can occur in Ethernet frames after the initial MAC-48 destination and source identifiers. Ethertypes are 16-bit identifiers appearing as the initial two octets after the MAC destination and source (or after a tag).

EtherType use implies the use of the IEEE Assigned EtherType Field with IEEE Std 802.3, 1998 Edition Local and Metropolitan Area Networks. The EtherType Field provides a context for interpretation of the data field of the frame (protocol identification). Several well-known protocols already have an EtherType Field.

The IEEE 802.3, 1998 Length/EtherType Field, originally known as EtherType, is a two-octet field. When the value of this field is greater than or equal to 1536 decimal (0600 hexadecimal) the EtherType Field indicates the nature of the MAC client protocol (EtherType interpretation). The length and EtherType interpretations of this field are mutually exclusive.

Communication

In IPv6, any packet exchange among nodes that requires that the address of each node used in the exchange remain the same for the duration of the packet exchange. Examples are a TCP connection or a UDP request- response.

CoS

The QoS technique known as Class of Service (CoS) is a 3-bit field called the Priority Code Point (PCP) within an Ethernet frame header when using VLAN tagged frames as defined by IEEE 802.1Q. The PCP specifies a priority value of between 0 and 7 (inclusive) to be used by QoS disciplines to differentiate traffic. This technique is commonly referred to as IEEE 802.1p, but there is no IEEE standard or amendment under

that name; the technique is incorporated into the IEEE 802.1Q standard, which specifies the tag inserted into an Ethernet frame.

Eight different classes of service can be expressed with the 3-bit PCP field in an IEEE 802.1Q header added to the frame. The way traffic is treated when assigned to any particular class is undefined by the spec and is left to the implementation. The IEEE however has made some broad recommendations:

PCP	Priority	Acronym	Traffic Types
1	0 (lowest)	BK	Background
0	1	BE	Best Effort
2	2	EE	Excellent Effort
3	3	CA	Critical Applications
4	4	VI	Video, < 100 ms latency and jitter
5	5	VO	Voice, < 10 ms latency and jitter
6	6	IC	Internetwork Control
7	7 (highest)	NC	Network Control

Note that the above recommendation was revised in IEEE 802.1Q-2005, and it also differs from the original IEEE 802.1D-2004 recommendation. See also "QoS".

D

DA

(Destination Address); contrast SA.

DAD

(Duplicate Address Detection) - In IPv6, part of the NDP protocol that lets nodes check if an address is already in use.

DEI

DEI is an acronym for **D**rop **E**ligible **I**ndicator. It is a 1-bit field in the VLAN tag.

Deprecated address

In IPv6, an address assigned to an interface whose use is discouraged, but not forbidden. A deprecated address should no longer be used as a source address in new communications, but packets sent from or to deprecated addresses are delivered as expected. A deprecated address may continue to be used as a source address in communications where switching to a preferred address causes hardship to a specific upper-layer activity (e.g., an existing TCP connection).

DES

DES (**D**ata **E**ncryption **S**tandard) provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP (Dynamic Host Configuration Protocol) is a protocol 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 Relay

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 standalone switch it always equal 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 is equal the DHCP relay agents MAC address.

DHCP Snooping

DHCP Snooping is used to block intruders 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.

DMAC

(Destination MAC Address) A valid source MAC address, except for an address which has the lowest bit of the first byte set to '1'. These addresses, including the all 1's broadcast address FF:FF:FF:FF:FF:FF and the set of multicast addresses, are point-to-multipoint addresses and can never appear as the source address in an Ethernet frame. Note that a frame must be sent by a single source.
Each MAC header consists of three parts: 1. A 6-byte destination address, which specifies either a single recipient node (unicast mode), a group of recipient nodes (multicast mode), or the set of all recipient nodes (broadcast mode). 2. A 6-byte source address, which is set to the sender's globally unique node address. This may be used by the network layer protocol to identify the sender, but usually other mechanisms are used (e.g. ARP). Its main function is to allow address learning which may be used to configure the filter tables in a bridge.
3. A 2-byte type field, which provides a Service Access Point (SAP) to identify the type of protocol being carried.
See also "SMAC".

DMI

Diagnostic Monitoring Interface; the S4224 is capable of supporting connectors with DMI (SFF-8472) capability. All DMI events will trigger notification. An intrusion detection based on Rx Power level is available for triggering any drop in the Rx power.

DNS

DNS (Domain Name System) stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

DoS is an acronym for **D**enial of **S**ervice. In a DoS attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets. An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

DSCP

DSCP (Differentiated Services Code Point) is a field in the header of IP packets for packet classification purposes. In an IP header, a six-bit DSCP field specifies the per-hop behavior for a given flow of packets. Each packet is given one of 64 possible forwarding behaviors (known as per-hop behaviors, or PHBs) for a given set of packet travel rules. DSCP uses the first 6 bits in the ToS field of the IPv4 packet header. In many cases, DSCP has replaced the outdated Type of Service (TOS) field.

Dual stack

One of three options for migrating to IPv6 from an existing IPv4 network infrastructure (dual-stack network, tunneling, and translation).

E

E911

Enhanced 911 Emergency Call Service applicable in North America.

EAPOL

The key protocol in 802.1x is called ‘EAP over LANs’ (EAPOL), which is currently defined for Ethernet-like LANs including 802.11 wireless, as well as token ring LANs (including FDDI).

In 802.1X, the user is called the ‘supplicant’, the switch is the’ authenticator’, and the RADIUS server is the ‘authentication server’. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. Note that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

The authenticator acts like a ‘security guard’ to a protected network. The supplicant (client device) is not allowed access through the authenticator to the protected side of the network until the supplicant’s identity has been validated and authorized. The commonly used EtherType for EAPOL is 0x888E.

ECS

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

ECEs

(EVC Control Entries) The ECE ID identifies the ECE. Unique ECE IDs are automatically assigned to ECEs added. The possible range is from 1 through 128. See also “EVC”.

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

ELIN

Emergency Location Identification Number, a valid North America Numbering Plan format telephone number, supplied to the PSAP for ECS purposes.

E-LSP

An EXP-Inferred-PSC LSP PSC decision also based on EXP/TC bits. A single LSP can be used to support one or more OAs. Such LSPs can support up to eight BAs of a given FEC, regardless of how many OAs these BAs span. With such LSPs, the EXP field of the MPLS Shim Header is used by the LSR to determine the PHB to be applied to the packet. This includes both the PSC and the drop preference.

Such LSPs are referred to as "EXP-inferred-PSC LSPs" (E-LSP), since the PSC of a packet transported on this LSP depends on the EXP field value for that packet. The mapping from the EXP field to the PHB (i.e., to PSC and drop precedence) for a given such LSP, is either explicitly signaled at label set-up or relies on a pre-configured mapping. See IETF RFC 3270. See also “L-LSP”.

ENNI

(External Network-to-Network Interface) External Network to Network Interface; a reference point representing the boundary between two Operator MENs that are operated as separate administrative domains per MEF 26, 30. Previously “E-NNI”.

Epoch

The origin of a PTP timescale.

EPS / ELPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031 (Ethernet (Linear) Protection Switch). Rec. ITU-T G.8031/Y.1342 (11/2009) defines the automatic protection switching APS protocol and linear protection switching mechanisms for point-to-point VLAN-based ETH SNC (Subnetwork Connection) in Ethernet transport networks. Protection switching occurs based on detection of certain defects on the transport entities (working and protection) within the protected domain. These defects are discussed in ITU-T G.8021.

The G.8031 Recommendation specifies linear protection switching mechanisms to be applied to VLAN-based Ethernet networks as described in G.8010. Protection switching is a fully allocated survivability mechanism (‘fully allocated’ in that the route and bandwidth of the protection entity is reserved for a selected working entity). EPS provides a fast and simple survivability mechanism. It is easier for a network operator to understand the network status (e.g., active network topology) with EPS than with other survivability mechanisms such as RSTP.
G.8031 specifies linear 1+1 protection switching architecture and linear 1:1 protection switching architecture. The ETH-APS defined in Y.1731 is used as a signaling channel. G.8031 (2006) Amd. 1renamed EPS to ELPS.

ERP instance

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. Per ITU-T Rec.G.8032/Y.1344 (03/2010).

ERPS

ERPS is an abbreviation for Ethernet ring protection switching. Recommendation ITU-T G.8032/Y.1344 defines the automatic protection switching (APS) protocol and protection switching mechanisms for ETH layer Ethernet ring topologies. Included are details on Ethernet ring protection characteristics and architectures, and the Ring APS (R-APS) protocol. The protection protocol defined in this Recommendation enables protected point-to-point, point-to-multipoint and multipoint-to-multipoint connectivity within a ring or interconnected rings, called "multi-ring/ladder network" topology. The ETH layer ring maps to the physical layer ring structure.

The ERPS effort at ITU-T under G.8032 is to provide sub-50ms protection and recovery switching for Ethernet traffic in a ring topology and at the same time ensuring that there are no loops formed at the Ethernet layer. G.8032v1 supported a single ring topology and G.8032v2 supports multiple rings/ladder topology.

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 G.8032 provide highly reliable and stable protection; and avoid loops which would prove fatal to 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 basis of this RPS architecture are a) the principle of loop avoidance, and b) the use of learning, forwarding, and Filtering Database (FDB) mechanisms defined in the Ethernet flow forwarding function (ETH_FF).

Loop avoidance in an Ethernet Ring is done by guaranteeing that at all times, 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 Neighbor Node, may also participate in blocking or unblocking its end of the RPL.

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.

ERPS Performance

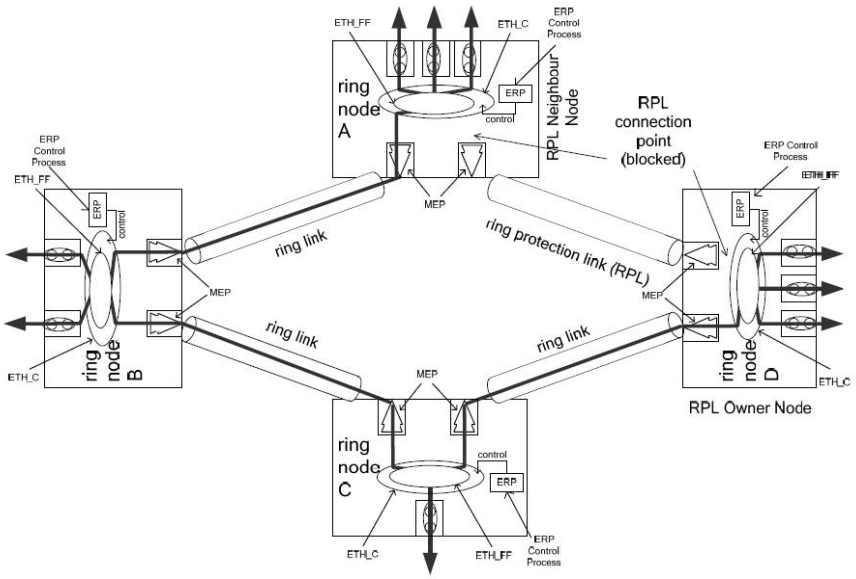
Note from Rec. ITU-T G.8032/Y.1344 (03/2010): “Ethernet ring protection switching performance: In an Ethernet ring, without congestion, with all Ethernet ring nodes in the idle state (i.e., no detected failure, no active automatic or external command, and receiving only "NR, RB" R-APS messages), with less than 1200 km of ring fibre circumference, and fewer than 16 Ethernet ring nodes, the switch completion time (transfer time as defined in [ITU-T G.808.1]) for a failure on a ring link will be less than 50 ms. On Ethernet rings under all other conditions, the switch completion time may exceed 50 ms (the specific interval is under study), to allow time to negotiate and accommodate coexisting APS requests. In case of interconnection of sub-rings with R-APS virtual channel to a major ring, the R-APS messages of the sub-ring that are inserted into the R-APS virtual channel take on performance characteristics (e.g., delay, jitter, packet drop probability, etc.) of the ring links and Ethernet ring nodes it crosses over the interconnected Ethernet ring. In this case, if the R-APS channel and R-APS virtual channel exceed the number of Ethernet ring nodes or fibre circumference defined above, the protection switching of the sub-ring may exceed 50 milliseconds. NOTE – The inclusion of the completion of FDB flush operation within the transfer time is for further study.”

ESP

The IP Encapsulating Security Payload (ESP) protocol provides a mix of security services in IPv4 and IPv6. ESP supports two modes of operation: tunnel mode and transport mode.
The ESP header is designed to provide a mix of security services in IPv4 and IPv6. ESP may be applied alone, in combination with AH, or in a nested fashion.
Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host. The ESP header is inserted after the IP header and before the next layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode). ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality. The set of services provided depends on options selected at the time of Security Association (SA) establishment and on the location of the implementation in a network topology. See IETF RFC 4303.

Ethernet ring

A collection of Ethernet ring nodes forming a closed physical loop whereby each Ethernet ring node is connected to two adjacent Ethernet ring nodes via a duplex communications facility. From ITU-T Rec.G.8032/Y.1344 (03/2010).



Ethernet ring node

A network element which implements at least the following functionalities:
a) One Ethernet connection function (ETH_C) with a dedicated Ethernet flow forwarding function (ETH_FF) for forwarding ring automatic protection switching (R-APS) control traffic.
b) Two ring ports, including ETHDi/ETH adaptation function at the ring maintenance entity group level (MEL).
c) Ethernet ring protection (ERP) control process controlling the blocking and unblocking of traffic over the ring ports. Per ITU-T Rec.G.8032/Y.1344 (03/2010).

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).

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame. See “Commonly Used EtherTypes” above.

EUI-64

The 64-bit Extended Unique Identifier (EUI-64) in IPv6.

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. Per MEF 6.1, EVC performance requires “At least one CoS is REQUIRED. MUST specify CoS ID, per section 6.8 of [2]. MUST list values for each of the following attributes {Frame Delay, Frame Delay Variation, Frame Loss Ratio, and Availability} for each CoS, where Not Specified (N/S) is an acceptable value.”

EXP

Experimental bits; in MPLS, the old name for “TC”.

F

Fast Leave

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.

FCS

(Frame Check Sequence) per MEF 8, 11, 12.

FEC (Forwarding Equivalence Class)

For any routing protocol to be able to survive, scalability problems must be resolved early on. To ensure scalability, flow states should be managed on aggregation and never on individual flows. MPLS ensures scalability supporting the aggregation using “Forwarding Equivalence Class” (FEC).

The LER is the place where aggregation is completed. The LER is responsible for classifying incoming packets and relating them to FECs. Each FEC is associated with an appropriate label and forwarding path. LER uses several modes to classify traffic. For example, using the packet destination adress and port in the table below:

Dest. Address	Dest. Port	FEC	Next Hop	Label	Instruction
201.20.3.4	80	B	x.x.x.x	65	Push
201.20.4.5	443	A	y.y.y.y	18	Push
209.11.9.1	25	IP	z.z.z.z	--	Native IP

Packets leaving the LER to go into the MPLS domain are forwarded using LSRs. To do this, the LSR looks just at labels on the MPLS packet and matches it with labels within its forwarding table. This forwarding table is called the LIB (Label Information Base). The LSR will push, pop, or swap labels and then forward packets according with LIB instructions.
A representation of such a table is shown below:

Label In	Port In	Label Out	Port Out	FEC	Instruction
80	G	67	B	B	Swap
27	A	28	C	M	Pop

Finally when the packet reaches another LER to leave the MPLS domain, the LER removes the MPLS header and forwards the packet to an IP network.

LER performs what is called the initial MF (multi-field) classification. It can map layer-2 to MPLS, MPLS to layer-3 and makes MF classification wit very fine granularity. This classification will decide which IP packets will be converted to MPLS packets, and which will traverse the router being untouched.

Pushing several labels instead of one lets us create a stack of labels, each one representing a network hierarchy. For example, suppose a packet enters an MPLS domain. When it enters the first network in the domain, the label *45* is pushed. The packet then travels through the domain using this first label. Routers will forward the packet following instructions given by label *45*. Then, somewhere, when the packet enters a second network within the same domain, a new label is pushed, i.e. label *56*. Now the packet will be forwarded using a different set of instructions which correspond to the label *56*. When the packet reaches the second network frontier, the last LER router pops the label *56* (really penultimate hop is used to do this) and forwards the packet again to the first network using its original label number *45*. This example is a 2-level hierarchy; other network hierarchy possibilities are nearly endless.

flow

A given type of traffic sent between a producer device through a network to an endpoint known as a consumer. As the traffic goes through the network, it “flows” through the network. See also "Per flow QoS".

Foreign master

An ordinary or boundary clock sending Announce messages to another clock that is not the current master recognized by the other clock.

FPGA

(Field-Programmable Gate Array) a chip that can be programmed in the field after manufacture.

FTP

FTP is an acronym for **F**ile **T**ransfer **P**rotocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

G

GAL

Generic Associated Channel Label (IETF RFC5586). Using MPLS Label value= 13 is used for OAM.

G-ACH

Generic Associated Channel (per IETF RFC5586)

GLAG

(Global Link Aggregation Group) is one of two supported types of Link Aggregation Groups. With GLAG, ports in a GLAG may reside on the same unit, up to two GLAGs are supported per stack, and each of the two GLAGs may consist of up to eight ports.
For both LLAGs and GLAGs, the egress port is chosen based on an 'aggregation code' that is calculated for the frame. This ensures that frames relating to a given frame flow are forwarded on the LLAG or GLAG member port, and thus do not risk being re-ordered. See also "LLAG".

Global address

In IPv6, an address with unlimited scope.

Grandmaster clock

Within a PTP domain, a clock that is the ultimate source of time for clock synchronization using the protocol.

H

HMAC

(Hash-based Message Authentication Code) - a specific construction that calculates a message authentication code (MAC) involving a cryptographic hash function in combination with a secret key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. Any cryptographic hash function (e.g., MD5 or SHA-1) may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly. The cryptographic strength of the HMAC depends on the cryptographic strength of the underlying hash function, the size of its hash output length in bits, and on the size and quality of the cryptographic key.

Host

In IPv6, any node that is not a router.

HTTP

HTTP (Hypertext Transfer Protocol) is a protocol that used to transfer or convey information on the World Wide Web (WWW). HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) is used to indicate a secure HTTP connection. HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP (Internet Control Message Protocol) is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

ICMPv6

(Internet Control Message Protocol version 6) is the implementation of the Internet Control Message Protocol (ICMP) for Internet Protocol version 6 (IPv6) defined in RFC 4443.[1] ICMPv6 is an integral part of IPv6 and performs error reporting, diagnostic functions (e.g., ping), and a framework for extensions to implement future changes. Several extensions are published to define new ICMPv6 message types and options for existing ICMPv6 message types. The Neighbor Discovery Protocol (NDP) is a node discovery protocol in IPv6 that replaces and enhances functions of ARP. Secure Neighbor Discovery Protocol (SEND) is an extension of NDP with extra security. Multicast Router Discovery (MRD) allows discovery of multicast routers.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

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.
Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. IGMP have three fundamental types of message as follows:

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit to be a member of a specific multicast group.

IGMP Querier

When a router sends IGMP Query messages onto a particular link, this router is called the 'Querier'. In order for IGMP, and thus IGMP snooping, to function, a multicast router must exist on the network and generate IGMP queries. The tables created for snooping (holding the member ports for a each multicast group) are associated with the querier. Without a querier the tables are not created and snooping will not work. Furthermore IGMP general queries must be unconditionally forwarded by all switches involved in IGMP snooping.[1] Some IGMP snooping implementations include full querier capability. Others are able to proxy and retransmit queries from the multicast router.

IGMP snooping

The process of listening to Internet Group Management Protocol (IGMP) network traffic. IGMP snooping, as implied by the name, is a feature that allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them. A switch will, by default, flood multicast traffic to all the ports in a broadcast domain (or the VLAN equivalent). Multicast can cause unnecessary load on host devices by requiring them to process packets they have not solicited. When purposefully exploited this is known as one variation of a denial-of-service attack. IGMP snooping is designed to prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. It provides switches with a mechanism to prune multicast traffic from links that do not contain a multicast listener (an IGMP client).
IGMP snooping allows a switch to only forward multicast traffic to the links that have solicited them. Essentially, IGMP snooping is a layer 2 optimization for the layer 3 IGMP. IGMP snooping takes place internally on switches and is not a protocol feature. Two standards organizations define IGMP snooping - the IEEE standardizes Ethernet switches, and the IETF standardizes IP multicast.

IMAP

IMAP (Internet Message Access Protocol) is a protocol for email clients to retrieve email messages from a mail server. IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

I-NNI

(Internal Network to Network Interface) per MEF 4. Internal NNI (this definition has not been implemented in any specification) per MEF 17.

Interconnection node

An Ethernet ring node which is common to two or more Ethernet rings or to a sub-ring and an interconnected network. At each interconnection node there may be one or more Ethernet rings that can be accessed through a single ring port and not more than one Ethernet ring that is accessed by two ring ports. The former set of Ethernet rings is comprised of sub-rings, whereas the latter Ethernet ring is considered a major ring, relative to this interconnection node. If the interconnection node is used to connect a (set of) sub-ring(s) to another network, then there is no Ethernet ring accessed by two ring ports. Per ITU-T Rec.G.8032/Y.1344 (03/2010).

Interface

In IPv6, a node's attachment to a link.

Interface identifier

In IPv6, a link-dependent identifier for an interface that is (at least) unique per link. Stateless address autoconfiguration combines an interface identifier with a prefix to form an address. In address autoconfiguration, an interface identifier is a bit string of known length. The exact length of an interface identifier and the way it is created is defined in a separate link-type specific document that covers issues related to the transmission of IP over a particular link type. In many cases, the identifier will be the same as the interface's link- layer address.

Invalid address

In IPv6, an address that is not assigned to any interface. A valid address becomes invalid when its valid lifetime expires. Invalid addresses should not appear as the destination or source address of a packet. In the former case, the internet routing system will be unable to deliver the packet, in the later case the recipient of the packet will be unable to respond to it.

IP

IP (Internet Protocol) is a protocol used for communicating data across an internet network. IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

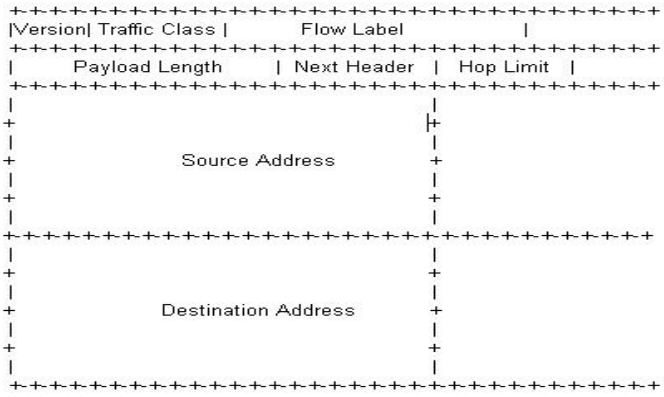
The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPv6

(Internet Protocol version 6) - The Version 6 IP protocol for Next Generation (IPng), a version of the Internet Protocol (IP) designed to succeed IPv4. The Internet operates by transferring data between hosts in small packets that are independently routed across networks as specified by an international communications protocol known as the Internet Protocol. Each host or computer on the Internet requires an IP address in order to communicate. The growth of the Internet has created a need for more addresses than are possible with IPv4. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with this long-anticipated IPv4 address exhaustion, and is described in Internet standard document RFC 2460, published in December 1998.[1] Like IPv4, IPv6 is an Internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks. While IPv4 allows 32 bits for an Internet Protocol address, and can therefore support 232 (4,294,967,296) addresses, IPv6 uses 128-bit addresses, so the new address space supports 2128 (approximately 340 undecillion or 3.4×1038) addresses. This expansion allows for many more devices and users on the internet as well as extra flexibility in allocating addresses and efficiency for routing traffic. It also eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion. See IETF RFC2460.

IPv6 Header

The IPv6 Header format is shown below - from RFC 2460 - IPv6 Specification (Dec. 1998).



The IPv6 header fields are:

- **Version**: The 4-bit Internet Protocol version number (6).
- **Traffic Class**: An 8-bit traffic class field.
- **Flow Label**: A 20-bit flow label.
- **Payload Length**: the 16-bit unsigned integer. The Length of the IPv6 payload (i.e., the rest of the packet following this IPv6 header, in octets. Note that any extension headers present are considered part of the payload (i.e., included in the length count.
- **Next Header**: An 8-bit selector that identifies the type of header immediately following the IPv6 header. Uses the same values as the IPv4 Protocol field.
- **Hop Limit**: An 8-bit unsigned integer decremented by 1 by each node that forwards the packet. The packet is discarded if the Hop Limit is decremented to zero.
- **Source Address**: The 128-bit address of the originator of the packet.
- **Destination Address**: The 128-bit address of the intended recipient of the packet (possibly not the ultimate recipient, if a Routing header is present).

A full IPv6 implementation also includes these six extension headers: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, and Encapsulating Security Payload headers. Unlike IPv4, IPv6 nodes are not required to enforce a maximum packet lifetime, which is why the IPv4 "Time to Live" field was renamed "Hop Limit" in IPv6.

IPMC

IPMC (IP MultiCast) provides a means to talk to a group of hosts (a multicast group), where each host has a different MAC address, and at the same time ensure that other hosts, which are not part of the multicast group, don't process the information. Broadcast packets make use of a broadcast MAC address (FF:FF:FF:FF:FF:FF), which includes setting the broadcast/multicast bit in the address. (Unicast packets are delivered to a specific recipient on an Ethernet or IEEE 802.3 subnet by setting a specific layer 2 MAC address on the Ethernet packet address.) A multicast address is associated with a group of interested receivers. In IPv4, addresses 224.0.0.0 through 239.255.255.255 (the former Class D addresses) are designated as multicast addresses.[3] IPv6 uses the address block with the prefix ff00::/8 for multicast applications. In either case, the sender sends a single datagram from its unicast address to the multicast group address and the intermediary routers take care of making copies and sending them to all receivers that have joined the corresponding multicast group.
IP multicast is a method of sending Internet Protocol (IP) datagrams to a group of interested receivers in a single transmission. It is often employed for streaming media applications on the Internet and private networks. The method is the IP-specific version of the general concept of multicast networking. It uses special reserved multicast address blocks in IPv4 and IPv6. In IPv6, IP multicast addressing replaces broadcast addressing as implemented in IPv4. The Linux commands ***ping*** and ***netstat*** are helpful when using IP multicast.
Ping commands can be used for multicast addresses by providing a multicast address as argument. Running ***netstat*** with the ***–g*** option on a Linux system displays the set of all multicast groups that the Linux system has joined.

IP Source Guard

IP Source Guard is a secure 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.

J

Jumbo frames

The S4224 supports jumbo frames. This frame size is set to 10056 bytes or jumbo mode by default. The frame size is configurable to any value from 1518-10056 bytes.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The **L**ink **A**ggregation **C**ontrol **P**rotocol allows bundling several physical ports together to form a single logical port. LACP is used by neighboring devices to agree on adding links to a Link Aggregation Group, and to maintain packet ordering within each LAG. LACP will form an aggregation when 2 or more S4224 ports are connected to the same partner.

LCI

Location Configuration Information.

LER (Label Edge Routing)

A Label Edge Router makes a decision on which label to prefix to a packet and forwards. Also, the last router in the path removes the label from the packet and forwards the packet based on the header.

Link

In IPv6, a communication facility or medium over which nodes can communicate at the link layer (i.e., the layer immediately below IPv6). Examples are Ethernets (simple or bridged); PPP links; X.25, Frame Relay, or ATM networks; and internet (or higher) layer "tunnels", such as tunnels over IPv4 or IPv6 itself.

Link-layer address

In IPv6, a link-layer identifier for an interface. Examples include IEEE 802 addresses for Ethernet links and E.164 addresses for ISDN links.

Link-local Address

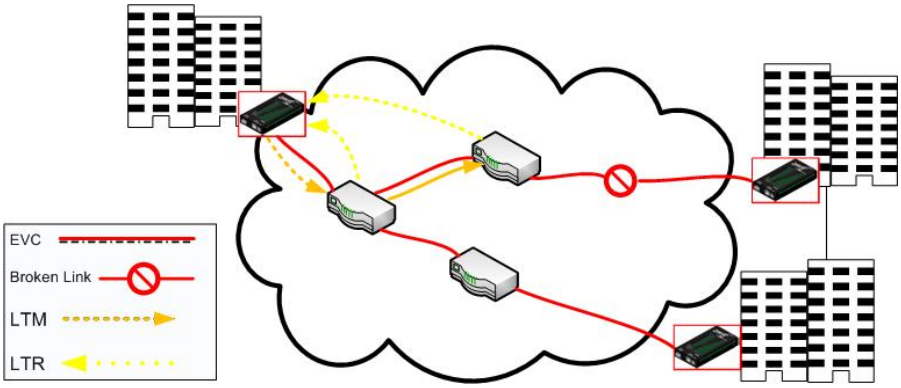
One of IPv6 addresses for local link usage. In IPv6, an address having link-only scope that can be used to reach neighboring nodes attached to the same link. All interfaces have a link-local unicast address.

Link MTU

The IPv6 Maximum Transmission Unit - the maximum packet size in octets that can be conveyed over a link.

Link Trace

Link Trace messages are Multicast frames that a MEP transmits to track the path (hop-by-hop) to a destination MEP. Each receiving MEP sends a Linktrace Reply (LTR) directly to the Originating MEP, and regenerates the Linktrace Message: Each Linktrace Message (LTM) is a CFM PDU initiated by a MEP to trace a path to a target MAC address, forwarded from MIP to MIP, up to the point at which the LTM reaches its target, a MEP, or can no longer be forwarded. Each MP along the path to the target generates an LTR. Each Linktrace Reply (LTR) is a unicast CFM PDU sent by an MP to a MEP, in response to receiving an LTM from that MEP. Linktrace Replies (LTRs) are carried in unicast frames. Linktrace Messages (LTMs) use addresses from the Linktrace Message Group Destination MAC Addresses table.



An LTM is used to signal to the MEP to transmit an LTM and to create an LTM entry in the MEP's Linktrace Database. The MA End Point can then be examined to determine whether or not the corresponding LTRs have been received by the MEP.
ETH-LT (Ethernet Link Trace) is an on-demand OAM function that can be used 1) to retrieve adjacency relationship between a MEP and a remote MEP or MIP, and 2) for Fault localization – when a fault (e.g., a link and/or a device failure) occurs, the sequence of MIPs and/or MEP will likely differ from the expected sequence. These differences provide information about the fault location.
ETH-LT request information is initiated in a MEP on an on-demand basis. After transmitting a frame with ETH-LT request information, the MEP expects to receive frames with ETH-LT reply information within a specified period of time. Network elements containing MIPs or MEPs and receiving the frame with ETH-LT request information respond selectively with frames containing ETH-LT reply information.

LLAG

(Local Link Aggregation Group) is one of two supported types of Link Aggregation Groups (same as Link Aggregation Group). With LLAG, all ports in an LLAG must reside on the same unit, any number of LLAGs may be configured for each unit in a stack, and each LLAG may consist of up to 16 ports. LLAGs are configured the same way as link aggregation groups for a standalone device (e.g., S4224).
For both LLAGs and GLAGs, the egress port is chosen based on an 'aggregation code' that is calculated for the frame. This ensures that frames relating to a given frame flow are forwarded on the LLAG or GLAG member port, and thus do not risk being re-ordered. See also "GLAG".

LLC

The IEEE 802.2 **L**ogical **L**ink **C**ontrol (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

LLDP

LLDP is an IEEE 802.1ab standard protocol. The **L**ink **L**ayer **D**iscovery **P**rotocol(LLDP) specified in this standard 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).

LLDP-MED

LLDP-MED Link Layer Discovery Protocol Media Endpoint Discovery. LLDP-MED is an extension of IEEE 802.1ab and is defined by the Telecommunication Industry Association (TIA-1057).

LLDPDU

Link Layer Discovery Protocol Data Unit, as defined in IEEE 802.1AB.

L-LSP

Label-Only-Inferred-PSC LSP. PSC decided based on label, not on EXP/TC bits.

LSP

MPLS Label Switched Path. S4224 LSP support includes LSR switching, up to two recursive layers of LSP (plus PW LER or LSP LSR) (LSP or PW can exist directly on the Ethernet port, inside one terminated LSP, or inside two terminated LSPs), and MPLS LSP OAM using GAL/G-ACH.

LOAM

(Link OAM) Ethernet Connectivity Fault Management (CFM) provided per IEEE 802.3ah OAM. The major features covered by this protocol are Discovery, Link Monitoring, Remote Fault Detection, and Remote Loopback. The S4224 NIDs support both Link layer OAM (LOAM, per IEEE 802.3–2005 Clause 57) and Service layer OAM (SOAM, per IEEE 802.1AG and Y.1731). Compare to “SOAM”.

LOC

LOC (Loss Of Connectivity) is detected by a MEP and indicates lost connectivity in the network. LOC can be used as a switch criteria by EPS.

LSP (Label Switched Path)

A label-switched path (LSP) is a path through an MPLS network, set up by a signaling protocol such as LDP, RSVP-TE, BGP or CR-LDP. The path is set up based on criteria in the FEC.
The path begins at a label edge router (LER), which makes a decision on which label to prefix to a packet based on the appropriate FEC. It then forwards the packet along to the next router in the path, which swaps the packet's outer label for another label, and forwards it to the next router. The last router in the path removes the label from the packet and forwards the packet based on the header of its next layer, for example IPv4. Due to the forwarding of packets through an LSP being opaque to higher network layers, an LSP is also sometimes referred to as an MPLS tunnel.
The router which first prefixes the MPLS header to a packet is called an ingress router. The last router in an LSP, which pops the label from the packet, is called an egress router. Routers in between, which need only swap labels, are called transit routers or label switch routers (LSRs).
Note that LSPs are unidirectional; they enable a packet to be label switched through the MPLS network from one endpoint to another. Since bidirectional communication is typically desired, the aforementioned dynamic signaling protocols can set up an LSP in the other direction to compensate for this.
When protection is considered, LSPs could be categorized as primary (working), secondary (backup) and tertiary (LSP of last resort). As described above, LSPs are normally P2P (point to point). A new concept of LSPs, which are known as P2MP (point to multi-point), was introduced recently. These are mainly used for multicasting purposes. See also “E-LSP” and “L-LSP”.

L-LSP

Label-Only-Inferred-PSC LSP: A separate LSP can be established for a single <FEC, OA> pair. With such LSPs, the PSC is explicitly signaled at the time of label establishment, so that after label establishment, the LSR can infer exclusively from the label value the PSC to be applied to a labeled packet. When the Shim Header is used, the Drop Precedence to be applied by the LSR to the labeled packet is conveyed inside the labeled packet MPLS Shim Header using the EXP field. When the Shim Header is not used (e.g., MPLS Over ATM), the Drop Precedence to be applied by the LSR to the labeled packet is conveyed inside the link layer header encapsulation using link layer specific drop precedence fields (e.g., ATM CLP).

Such LSPs are referred to as "Label-Only-Inferred-PSC LSPs" (L-LSP) since the PSC can be fully inferred from the label without any other information (e.g., regardless of the EXP field value). See IETF RFC 3270. See also “E-LSP”.

LSR (Label Switching Router)

Routers in between which swap labels and forwards based on new label. An MPLS router that performs routing based only on the label is called a Label-switched router (LSR) or transit router. This is a type of router located in the middle of an MPLS network and is responsible for switching the labels used to route packets.When an LSR receives a packet, it uses the label included in the packet header as an index to determine the next hop on the label-switched path (LSP) and a corresponding label for the packet from a lookup table. The old label is then removed from the header and replaced with the new label before the packet is routed forward.

M

MAC Swap

In SOAM testing, MEPs need to know about the device on the other side. They perform a MAC Swap so they can automatically populate the remote MAC Address to the test parameters. This is performed in Layer 2.
See the S4224 **Configuration** > **MEP** menu path description.

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.
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 switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

Major ring

The Ethernet ring that is connected on two ports to an interconnection node. From ITU-T Rec.G.8032/Y.1344 (03/2010).

Master clock

In the context of a single PTP communication path, a clock that is the source of time to which all other clocks on that path synchronize. A system of 1588 clocks may be segmented into regions separated by boundary clocks. Within each region there will be a single clock, the master clock, serving as the primary source of time. These master clocks will in turn synchronize to other master clocks and ultimately to the grandmaster clock.

MD5

MD5 (**M**essage-**D**igest algorithm **5** is a message digest algorithm used in a cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm. MD5 is an authentication protocol; one of two cryptography methods used for S4224 user authentication. MD5 is a widely used cryptographic hash function with a 128-bit hash value. Specified in RFC 1321, MD5 is used in a wide range of security applications, and is also commonly used to check file integrity. However, it has been shown that MD5 is not collision resistant; as such, MD5 is not suitable for applications like SSL certificates or digital signatures that rely on this property. MD5 was designed by Ron Rivest in 1991 to replace the earlier hash function MD4. See also “SHA”.

ME

(Maintenance Entity) An entity that requires management and is a relationship between two maintenance entity group (MEG) end points. MEs in Ethernet networks can nest but not overlap.

MED

Media Endpoint Discovery.

MEG

(Maintenance Entity Group) A ME Group (MEG) consists of the MEs that belong to the same service inside a common OAM domain.

MEG Level

The MEG Level is used to distinguish between OAM frames belonging to different nested MEs. MEs belonging to the same MEG share a common MEG Level. Eight MEG Levels have been identified for the purposes of Ethernet OAM.

When a Subscriber, Service Providers, and Network Operators share the MEG Levels space, allocation of MEG Levels can be negotiated between the various roles involved. A default allocation of MEG Levels is such that Service OAM frames for a Subscriber ME use MEG Level 7, 6 or 5; Service OAM frames for an EVC ME use MEG Level 3 or 4 as EVC ME belongs to a Service Provider OAM Domain; and Operator MEs use MEG Levels 2, 1, or 0. The MEG Levels used for UNI ME and NNI ME default to 0. Note that this default allocation of MEG Level space between Subscribers, Service Providers and Operators could change based on a mutual agreement between them.
MEG level of a MEP (0-7). The defaults per MEF 30 are:

MEG	Default MEG Level	Suggested Use (MEF 30)
Subscriber MEG	6	Subscriber monitoring of an Ethernet service.
Test MEG	5	SP isolation of subscriber reported problems.
EVC MEG	4	SP monitoring of provided service.
Service Provider MEG	3	SP Monitoring of Service Provider network.
Operator MEG	2	Netw. Operator monitoring of the portion of a network.
UNI MEG	1	Service Provider monitoring of a UNI.
ENNI MEG	1	Network Operators' monitoring of an ENNI.

(where SP = Service Provider)
Note: Assignment of numerical MEG Levels to 'subscriber' (or customer) role, Service Provider role, and Operator role is somewhat arbitrary since those terms imply business relationships that cannot be standardized. For example, a 'subscriber' (or customer) may also be an Operator seeking a service from another Operator. The MEG Level default values are consistent with a shared MEG Level model across Subscriber, Operators, and Service Providers.
Note: The MEF and Broadband Forum (BBF) are not aligned on the use of MEG Level 5. If interworking between an MEF compliant implementation and a BBF compliant implementation is required, an agreement on the use of MEG Level 5 is required between the two parties.

MEP

A MEP (Maintenance Entity Endpoint) is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).
A MEP (Maintenance end point) is an inward-facing point at the edge of the domain that defines the boundary and confines CFM messages within these boundaries. Inward facing means that they communicate through the relay function side, not the wire side (connected to the port). See also MIP, Down MEP, and Up MEP.
A MEG End Point (MEP) is a provisioned OAM reference point which can initiate and terminate proactive OAM frames. A MEP can also initiate and react to diagnostic OAM frames. A Point-to-Point EVC has two MEPs, one on each end point of the ME. A Multipoint-to-Multipoint EVC of *n* UNIs has *n* MEPs, one on each end point.

MIP

(Maintenance intermediate point) – A point internal to a domain, not at the boundary, that responds to CFM only when triggered by trace route and loopback messages. MIPs forward CFM frames received from MEPs and other MIPs, drop all CFM frames at a lower level, and forward all CFM frames at a higher level, regardless of whether they are received from the relay or wire side.
A MEG Intermediate Point (MIP) is a provisioned OAM reference point that can react to diagnostic OAM frames initiated by MEPs. A MIP does not initiate proactive or diagnostic OAM frames. See also “MEP”.

Mirroring

For debugging network problems or monitoring network traffic, the S4224 can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.) Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for **M**ulticast **L**istener **D**iscovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLD is a component of the Internet Protocol Version 6 (IPv6) suite, and is used by IPv6 routers to discover multicast listeners on a directly attached link (much as IGMP is used in IPv4). MLD 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 was updated by RFC 4604. Windows Vista and later support MLDv2. FreeBSD 8 supports MLDv2. The Linux kernel has supported MLDv2 since v 2.5.68.

MLD snooping

With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list of ports is created by 'snooping' IPv6 multicast control packets. In IPv6, MLD snooping performs a similar function to the IGMP snooping used in IPv4.

MPLS (MultiProtocol Label Switching)

MPLS is a scalable, protocol-independent transport. In an MPLS network:

- Data packets are assigned labels.
- Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself.
- Directs data from one network node to the next based on short path labels rather than long network addresses
- MPLS operates at a layer that is generally considered to lie between traditional definitions of layer 2 (data link layer) and layer 3 (network layer), and thus is often referred to as a "layer 2.5" protocol.
- The labels identify virtual links (paths) between distant nodes rather than endpoints.

MPLS-TP (MPLS Transport Profile)

MPLS-TP is a simplified version of MPLS for transport networks with some of the MPLS functions turned off, such as Penultimate Hop Popping (PHP), Label-Switched Paths (LSPs) merge, and Equal Cost Multi Path (ECMP). MPLS-TP does not require MPLS control plane capabilities and enables the management plane to set up LSPs manually.

MSTI

An MSTI (**M**ultiple **S**panning **T**ree **I**nstance) is typically one of the uplink ports that connects to one of the gateway devices. Valid MSTI ID values are from 0 through 4094. MSTI information can include VLAN mapping, bridge priority, port priority, and cost. MSTP allows formation of MST regions that can run multiple MST instances (MSTI). Multiple regions and other STP bridges are interconnected using one single common spanning tree (CST). Unlike some proprietary per-VLAN spanning tree implementations, MSTP includes all of its spanning tree information in a single BPDU format. This reduces the number of BPDUs required on a LAN to communicate spanning tree information for each VLAN, and also ensures backward compatibility with RSTP (and effectively, classic STP too). MSTP does this by encoding additional region information after the standard RSTP BPDU as well as a number of MSTI messages (0 to 64 instances; many bridges support fewer). Each of these MSTI configuration messages conveys the spanning tree information for each instance. Each instance can be assigned a number of configured VLANs, and frames (packets) assigned to these VLANs operate in this spanning tree instance whenever they are inside the MST region. To avoid conveying their entire VLAN to spanning tree mapping in each BPDU, bridges encode an MD5 digest of their VLAN-to-instance table in the MSTP BPDU. This digest is then used by other MSTP bridges, along with other administratively configured values, to determine if the neighboring bridge is in its MST region. See also "CIST".

Multicast address

In IPv6, an identifier for a set of interfaces (typically belonging to different nodes). A packet sent to a multicast address is delivered to all interfaces identified by that address.

MVR

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 it/them (Wikipedia).

N

NAS

The NAS (**N**etwork **A**ccess **S**erver) is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NDP

(Neighbor Discovery Protocol) - a protocol in the Internet Protocol Suite used with IPv6. NDP operates in the Link Layer and is responsible for address autoconfiguration of nodes, discovery of other nodes on the link, determining the Link Layer addresses of other nodes, duplicate address detection, finding available routers and DNS servers, address prefix discovery, and maintaining reachability information about the paths to other active neighbor nodes per IETF RFC 4861.

Neighbors

Nodes attached to the same link. Per IETF RFC 2461, Neighbor Discovery for IPv6 is done by Sending Router Advertisements and processing Router Solicitation.

NENA

National Emergency Number Association, the body responsible for evolution of public ECS architectures in North America.

NetBIOS

NetBIOS (Network Basic Input/Output System) is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN). The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS (Network File System) allows hosts to mount partitions on a remote system and use them as though they are local file systems. NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NID

Network Interface Devices - a NID is an effective way of providing operational and capital savings to service providers. A NID installs at the customer premise and provides a demarcation point between the service provider and customer's network. NIDs allow for end-to-end Operations, Administration and Maintenance (OAM) functionality for the service provider. The basic functions, such as loopback testing and remote fault isolation, in the NID provide service providers a number of benefits, including: reduced truck rolls, fewer test sets in the field, and increased reliability. The result of this for the service provider is a reduction in OpEx and CapEx while providing a faster return on investment (ROI).
While the operational savings of NIDs can be shown with their features and capabilities for remote troubleshooting, easy installation and SLA monitoring to reduce SLA penalties, it is important for service providers to be aware of the additional revenue streams and services that can be achieved when using a NID at the demarcation point. NIDs have advanced features such as bandwidth allocation, QoS, VLAN and other features that allow the service provider the capability to provide tiered service offerings to customers.

NMS

Network Management System. Contrast “EMS”.

NNI

(Network to Network Interface) In carrier Ethernet, the demarcation / peering point between service providers (ENNI) or between service provider internal networks (I-NNI), per MEF 3, 12, 17, 4, 30, 31.

Node

In IPv6, a device that implements IPv6.

Non-revertive mode

In non-revertive mode of unidirectional protection switching operation, in conditions where working traffic is being transmitted via the protection entity, if local protection switching requests
have been previously active and now become inactive, a local "do-not-revert state" is entered. Since this state now represents the highest priority local request, it is indicated on the transmitted "request/state" information and maintains the switch, preventing reversion back to the released bridge/selector position in non-revertive mode under no-request conditions. With bidirectional protection switching operation, a local do-not-revert state is entered when there is no higher priority of request received from the far end than that of the do-not-revert state, or when both the local state and far-end state are NR with the requested signal number 1.
Generally, Revertive operation is useful when the working transport entity is more optimized or the protection transport entity carries best effort traffic; Non-revertive operation can minimize the number of switching and service outage time. See also “Revertive mode”.

NTP

NTP (Network Time Protocol) is a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

OAM

OAM (Operation Administration and Maintenance) protocol is described in ITU-T Y.1731 and is used to implement carrier ethernet functionality. MEP functionality like CC and RDI is based on this. The S4224 provides configuration and monitoring of two types of Ethernet OAM:
1) end-to-end service OAM (SOAM) per IEEE 802.1ag and ITU-T Y.1731, to let Ethernet service providers monitor their services proactively, measure end-to-end performance, and guarantee that the customers receive the contracted SLA. Fault monitoring and performance measurement include frame delay, frame delay variation, frame loss and availability.
2) single segment Link OAM (LOAM) per IEEE 802.3ah for remote management and fault indication, including remote loopback, dying gasp, and MIB parameter retrieval.

OID

(Object IDentifier) Many standards define certain objects that require unambiguous identification, which can be achieved by ‘registration’. Registration is the assignment of an object identifier (OID) to an object in a way which makes the assignment available to interested parties. It is carried out by a registration authority. Registration can be effected by publishing in the standard the names and the corresponding definitions of object. Such a mechanism requires amendment of the standard for each registration, and hence is not appropriate in cases where the registration activity is high. Alternatively, registration can be affected by letting organizations act as registration authorities to perform registration on a flexible basis.

The registration tree is managed in a completely decentralized way (a node gives full power to its children) and it is impossible to be exhaustive (particularly world-wide). The registration tree is defined and managed following the ITU-T X.660 & X.670 Recommendation series (or the ISO/IEC 9834 series of International Standards).

One-step clock

A clock that provides time information using a single event message.

Optional TLVs

An LLDP frame contains multiple TLVs. For some TLVs it is configurable if the S4224 includes the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

Ordinary clock

A clock that has a single Precision Time Protocol port in a domain and maintains the timescale used in the domain. It may serve as a source of time (i.e., be a master clock), or may synchronize to another clock (i.e., be a slave clock). An ordinary clock is a 1588 clock with a single PTP port.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

P

Packet

An IPv6 header plus payload.

Parent clock

The master clock to which a clock is synchronized.

Path MTU

The minimum IPv6 link MTU of all the links in a path between a source node and a destination node.

Path Cost

A path cost value is given to each port. The cost is usually based on 802.1d guidelines. According to the original specification, cost is 1,000 Mbps (1 gigabit per second) divided by the bandwidth of the segment connected to the port. Therefore, a 10 Mbps connection would have a cost of (1,000/10) = 100.
A ‘path cost’ is an administratively assigned value for the contribution of a port to the path cost of paths toward the spanning tree root. A value of '0' assigns the automatically calculated default Path Cost value to the port (the default Path Cost). This complements the object dot1dStpPortPathCost or dot1dStpPortPathCost32, which returns the operational value of the path cost.
Typical STP path costs are shown below for certain data rates.

Data rate	STP Cost (802.1D-1998)	RSTP Cost (802.1W-2001)
4 Mbps	250	5,000,000
10 Mbps	100	2,000,000
16 Mbps	62	1,250,000
100 Mbps	19	200,000
1 Gbps	4	20,000
2 Gbps	3	10,000
10 Gbps	2	2,000

The recommended values for any intermediate link speed can be calculated as 20,000,000,000/(Link Speed in Kb/s). Limiting the range of the Path Cost parameter to 1-200,000,000 ensures that the accumulated Path Cost cannot exceed 32 bits over a concatenation of 20 hops.

PCP

PCP (Priority Code Point) is a 3-bit field storing the priority level for the 802.1Q frame (also known as User Priority.)

PD

PD (Powered Device) in a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PDU

(Protocol Data Units) 1. Information that is delivered as a unit among peer entities of a network and that may contain control information, address information or data. 2. In a layered system, a unit of data which is specified in a protocol of a given layer and which consists of protocol control information and possibly user data of that layer.

Peer-to-peer transparent clock

A transparent clock that, in addition to providing Precision Time Protocol event transit time information, also provides corrections for the propagation delay of the link connected to the port receiving the PTP event message. In the presence of peer-to-peer transparent clocks, delay measurements between slave clocks and the master clock are performed using the peer-to-peer delay measurement mechanism.

Per flow QoS

The ability to identify a traffic flow, enable rules on how that specific flow should be treated, and then define how the flow should behave when forwarded with other traffic flows. See also "flow".

PHY

PHY (Physical Interface Transceiver) is the device that implements the Ethernet physical layer per IEEE-802.3.

PIC

(Peripheral interface controller) a family of specialized microcontroller chips.

PING

The ping program sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected. `Ping` uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

Pipe Model

One of three different models defined in RFC 3270, and which define, for example, inheritance of TTL and EXP/TC in the label stack during push and pop. TTL inheritance is defined in IETF RFC 4343. See also "Short Pipe Model" and "Uniform Model".

PoE

PoE (Power Over Ethernet) is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

Preferred address

In IPv6, an address assigned to an interface whose use by upper layer protocols is unrestricted. Preferred addresses may be used as the source (or destination) address of packets sent from (or to) the interface.

Preferred lifetime

In IPv6, the length of time that a valid address is preferred (i.e., the time until deprecation). When the preferred lifetime expires, the address becomes deprecated.

Private VLAN

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN (PVLAN).

PSC

Per Hop Behavior Scheduling Class; IETF RFC 3140 defines a binary encoding to uniquely identify PHBs and/or sets of PHBs in protocol messages for cases where it is necessary or desirable to identify a set of PHBs in a protocol message, such as a message negotiating bandwidth management or path selection, especially when such messages pass between management domains.

PTP

PTP (Precision Time Protocol) is a network protocol for synchronizing the clocks of computer systems.

PW

(Pseudowire): An MPLS-TP Provider Edge (PE) router is an MPLS-TP LSR that adapts client traffic and encapsulates it to be transported over an MPLS-TP LSP. Encapsulation may be as simple as pushing a label, or it may require the use of a pseudowire.

The term Provider Edge refers to the node's role within a provider's network. A provider edge router resides at the edge of a given MPLS-TP network domain, in which case it has links to another MPLS-TP network domain or to a CE, except for the case of a pseudowire switching provider edge (S-PE) router, which is not restricted to the edge of an MPLS-TP network domain.

The MPLS-TP native service adaptation functions interface the client layer network service to MPLS-TP. For pseudowires, these adaptation functions are the payload encapsulation described in Section 4.4 of RFC3985 and Section 6 of RFC5659.

MPLS-TP uses IETF-defined pseudowires to emulate certain services, for example, Ethernet, Frame Relay, or PPP / High-Level Data Link Control (HDLC). A list of PW types is maintained by IANA in the "MPLS Pseudowire Type" registry. See https://tools.ietf.org/html/rfc4446. Specific examples include:

0x0001 = Frame Relay DLCI (Martini Mode), **0x0004** = Ethernet Tagged Mode, **0x0005** = Ethernet, **0x0006** = HDLC, **0x0007**= PPP, **0x0008** = SONET/SDH Circuit Emulation Service Over MPLS, **0x0010** = SONET/SDH Circuit Emulation over Packet, and **0x0015** = CESoPSN basic mode.

Q

QCE

QCE (QoS Control Entry) describes QoS class associated with a particular QCE ID. There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of four different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

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. The privileges determine specific traffic object to specific QoS class.

QL

QL, in SyncE, is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

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. QoS is the set of techniques to manage network resources.
When discussing QoS features:

- "Packets" carry traffic at Layer 3.
- "Frames" carry traffic at Layer 2 (Layer 2 frames carry Layer 3 packets).
- "Classification" is the selection of traffic to be marked.
- "Marking" (per RFC 2475) is the process of setting a Layer 3 DSCP value of a packet.
- "Policing" is limiting bandwidth used by a flow of traffic; policing can either mark or drop traffic.

R

RAL

Router Alert Label (IETF RFC3032). Using MPLS Label value = 1.

R-APS

R-APS is an acronym for Ring APS. Per G.8032v1, in ERPS there is a central node called the 'RPL Owner Node' which blocks one of the ports to ensure that there is no loop formed for the Ethernet traffic. The link blocked by the RPL Owner node is called the Ring Protection Link or RPL. The node at the other end of the RPL is known as RPL Neighbour Node. It uses R-APS control messages to coordinate the activities of switching on/off the RPL link.

Any failure along the ring triggers an R-APS(SF) (R-APS signal fail) message along both directions from the nodes adjacent to the failed link after these nodes have blocked the port facing the failed link. On obtaining this message, RPL owner unblocks the RPL port. Note that a single link failure anywhere in the ring ensures a loop free topology.

During the recovery phase when the failed link gets restored, the nodes adjacent to the restored link send R-APS (NR) (R-APS no request) messages. On obtaining this message, the RPL owner blocks the RPL port and then sends a R-APS (NR,RB) (R-APS no request, root blocked) messages. This causes all other nodes other than the RPL Owner in the ring to unblock all of the blocked ports.

This 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 support field maintenance scenarios.

R-APS virtual channel

The Ring Automatic Protection Switching (R-APS) channel connection between two interconnection nodes of a sub-ring in (an)other Ethernet ring(s) or network(s). Its connection characteristics (e.g., path, performance, etc.) are influenced by the characteristics of the network (e.g., Ethernet ring) providing connectivity between the interconnection nodes. From ITU-T Rec.G.8032/Y.1344 (03/2010).

RARP

RARP (**R**everse **A**ddress **R**esolution **P**rotocol) is a protocol used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS (**R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice) is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI

RDI (Remote Defect Indication) is an OAM function used by a MEP to indicate a defect detected to the remote peer MEP. The IEEE Remote Defect Indication (RDI) is a single bit carried by the CCM. The absence of RDI in a CCM indicates that the transmitting MEP is receiving CCMs from all configured MEPs. A MEP can use ITU-T ETH-RDI to notify its peer MEPs that it detects a defect condition. ETH-RDI is used only if ETH-CC transmission is enabled. ETH-RDI is used in single-ended fault management and in contributing to far-end performance monitoring. A MEP in a defect condition transmits frames with ETH-RDI information. When a MEP receives frames with ETH-RDI information it determines that its peer MEP has encountered a defect condition
A MEP, on detecting a defect condition with its peer MEP, sets the RDI field in the CCM frames for the duration of the defect condition. CCM frames are transmitted periodically based on the CCM transmission period when the MEP is enabled for CCM frames transmission. When the defect condition clears, the MEP clears the RDI field in the CCM frames in subsequent transmissions.

Reversion Time (WTR time)

In revertive mode, the Reversion Time is the difference between the repair instant of the original resource and the Reversion Instant.

Revertive Mode

Protection is in revertive mode if, after a resource failure and its subsequent repair, the network automatically reverts to using this initial resource. The protection is in non-revertive mode otherwise. Automatic reversion may include a reversion timer (i.e., the Wait To Restore), which delays the time of reversion after the repair.
In Revertive mode of unidirectional protection switching operation, in conditions where working traffic is being received via the protection entity, if local protection switching requests have been previously active and now become inactive, a local wait-to-restore state is entered. Since this state now represents the highest priority local request, it is indicated on the transmitted "request/state" information and maintains the switch. With bidirectional protection switching, a local wait-to-restore state is entered only when there is no higher priority of request received from the far end than that of the wait-to-restore state. This state normally times out and becomes a no request state after the wait-to-restore timer has expired. The wait-to-restore timer is deactivated earlier if any local request of higher priority pre-empts this state. A switch to the protection entity may be maintained by a local wait-to-restore state or by a remote request (wait-to-restore or other) received via the "request/state" information. So, in a case
where a bidirectional failure for a working entity has occurred and subsequent repair has taken place, the bidirectional reversion back to the working entity does not take place until both wait-to-restore timers at both ends have expired. See also “Non-revertive mode”.

Ring MEL

The Maintenance Entity Group (MEG) Level providing a communication channel for ring automatic protection switching (R-APS) information. From ITU-T Rec.G.8032/Y.1344 (03/2010).

Ring Protection Link (RPL)

The ring link that under normal conditions, i.e., without any failure or request, is blocked (at one or both ends) for traffic channel, to prevent the formation of loops. From ITU-T Rec.G.8032/Y.1344 (03/2010).

RPL Neighbour node

The RPL neighbour node, when configured, is an Ethernet ring node adjacent to the RPL that is responsible for blocking its end of the RPL under normal conditions (i.e., the ring is established and no requests are present in the ring) in addition to the block by the RPL owner node. However, it is not responsible for activating the reversion behaviour. From ITU-T Rec.G.8032/Y.1344 (03/2010). Contrast “RPL Owner Node”.

RPL Owner node

The RPL owner node is an Ethernet ring node adjacent to the RPL that is responsible for blocking its end of the RPL under normal conditions (i.e., the ring is established and no requests are present in the ring). Furthermore, it is responsible for activating reversion behaviour from protected or manual switch/forced switch (MS/FS) conditions. From ITU-T Rec.G.8032/Y.1344 (03/2010). Contrast “RPL Neighbor Node”.

Router

In IPv6, a node that forwards IPv6 packets not explicitly addressed to itself.

Router Port

A port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the **R**apid **S**panning **T**ree **P**rotocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SA

(Source Address); contrast DA.

SAMBA

Samba is a program running under UNIX-like operating systems that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.

Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2. Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".

SFP

Small Form Factor Pluggable module (1-4Gbps).

SFP+

Small Form Factor Pluggable Plus module (8-10Gbps).

SHA

SHA (**S**ecure **H**ash **A**lgorithm) is designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length. SHA is an authentication protocol; one of two cryptography methods used for S4224 user authentication. SHA-1 is a cryptographic hash function designed by the National Security Agency (NSA) and published by the NIST as a U.S. FIPS standard. SHA-1 is part of many widely accepted security applications and protocols (e.g., TLS, SSL, PGP, SSH, S/MIME, and IPSec). See also “MD5”.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

Short Pipe Model

One of three different models defined in RFC 3270, and which define, for xample, inheritance of TTL and EXP/TC in the label stack during push and pop. TTL inheritance is defined in RFC 4343. See also "Pipe Model" and "Uniform Model".

Site-local Address

An IPv6 addresses for local site only. In IPv6, an address having scope that is limited to the local site.

SMAC

(Source MAC Address) The 12 hex digits of a source MAC address consist of the first/left 6 digits (which should match the vendor of the Ethernet NIC) and the last/right 6 digits which specify the interface serial number for that interface controller vendor. See also "DMAC". The list below identifies some of the blocks of assigned vendor MAC addresses (i.e. the first 3 bytes of a MAC source address).
00000C Cisco
00000E Fujitsu
00000F NeXT
00001D Cabletron
000022 Visual Technology
00002A TRW
00005A S & Koch
00005E IANA
000065 Network General
00006B MIPS
000093 Proteon
08005A IBM
080067 Comdesign
080069 Silicon Graphics
08007C Vitalink TransLAN III
080080 XIOS

080086 Imagen/QMS
080087 Xyplex terminal servers
080089 Kinetics AppleTalk-Ethernet interface
080090 Retix Inc Bridges

SMTP

SMTP (Simple Mail Transfer Protocol) is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP (Simple Network Management Protocol) is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow 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 implementing SNMP.

SNTP

SNTP (Simple Network Time Protocol) is a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SOAM

(Service OAM) provides Ethernet Connectivity Fault Management (CFM) per IEEE 802.1AG. Ethernet CFM comprises three protocols that work together to help administrators debug Ethernet networks: continuity check, link trace and loopback protocols. The S4224 supports both Link layer OAM (LOAM, per IEEE 802.3–2005 Clause 57) and Service layer OAM (SOAM, per IEEE 802.1AG and Y.1731).Compare to ‘LOAM’.

Solicited-node multicast address

In IPv6, a multicast address to which Neighbor Solicitation messages are sent. The algorithm for computing the address is given in Discovery.

Spanning Tree

The original spanning-tree protocol (STP) was created to prevent broadcast storms and other unwanted side effects of looping. Since, STP has been standardized as the 802.1d specification by the IIEEE.
A spanning tree uses a spanning-tree algorithm (STA) to sense that the switch has more than one way to communicate with a node, then determine the best way, and then block out all other paths. The STA also keeps track of the other paths, in case the primary path becomes unavailable.
Each switch is assigned a group of IDs - one for the switch itself and one for each port on the switch.
A switch's bridge ID (BID) is 8 bytes long and contains a bridge priority (2 bytes) along with one of the switch's MAC addresses (6 bytes). Each port ID is 16 bits long with two parts - a 6-bit priority setting and a 10-bit port number. A 'path cost' value is assigned to each port. See also "Path Cost".

SPME

TCM can be supported by the instantiation of a sub-path maintenance element (SPME) that has a 1:1 relationship with the monitored connection. See IETF RFC 6371 section 3.2. The SPME is then monitored using normal label switched path (LSP) monitoring. When an SPME is established between non-adjacent nodes, the edges of the SPME become adjacent at the client sub-layer network and any intermediate node that were previously in between becomes an intermediate node for the SPME. See also "TCM".

SSID

Service **S**et **Id**entifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their

SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (Wikipedia).

SSH

SSH (**S**ecure **Sh**ell) is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

SSM in SyncE is an abbreviation for Synchronization Status Message and contains a QL indication.

SSM

SSM (Source-Specific Multicast) IP version 4 (IPv4) addresses in the 232/8 (232.0.0.0 to 232.255.255.255) range are designated as source-specific multicast (SSM) destination addresses and are reserved for use by source-specific applications and protocols. For IP version 6 (IPv6), the address prefix FF3x::/32 is reserved for source-specific multicast use. IETF RFC 4607 defines an extension to the Internet network service that applies to datagrams sent to SSM addresses and defines the host and router requirements to support this extension.

Source-specific multicast (SSM) is a method of delivering multicast packets in which the only packets that are delivered to a receiver are those originating from a specific source address requested by the receiver. By so limiting the source, SSM reduces demands on the network and improves security. SSM requires that the receiver specify the source address and explicitly excludes the use of the (*,G) join for all multicast groups in RFC 3376, which is possible only in IPv4's IGMPv3 and IPv6's MLDv2.

The burden of source discovery on the network can be significant with a large number of sources. In the SSM model, in addition to the receiver expressing interest in traffic to a multicast address, the receiver expresses interest in receiving traffic from only one specific source sending to that multicast address. This relieves the network of discovering many multicast sources and reduces the amount of multicast routing information that the network must maintain. SSM requires support in last-hop routers and in the receiver's operating system. SSM support is not required in other network components, including routers and even the sending host. Interest in multicast traffic from a specific source is conveyed from hosts to routers using IGMPv3 as specified in RFC 4607. SSM destination addresses must be in the range of 232.0.0.0/8 for IPv4 or FF3x::/96 for IPv6.

SSM identifies a set of multicast hosts not only by group address but also by source. An SSM group, called a ‘channel’, is identified as (S,G) where S is the source address and G is the group address.

Stateless auto-configuration

A process to get IPv6 addresses from IPv6 standards.

Stateless

A communications protocol that treats each request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of requests and responses.
A stateless protocol does not require the server to retain session information or status about each communications partner for the duration of multiple requests. An example of a stateless protocol is the Hypertext Transfer Protocol (HTTP) which is the foundation of data communication for the World Wide Web.

The stateless design simplifies the server design because there is no need to dynamically allocate storage to deal with conversations in progress. If a client dies in mid-transaction, no part of the system needs to be responsible for cleaning the present state of the server. A disadvantage of statelessness is that it may be necessary to include additional information in every request, and this extra information will need to be interpreted by the server. An example of a stateless protocol is HTTP. The protocol provides no means of storing a user's data between requests. As a work-around, HTTP Servers implement various session management methods, typically utilizing a unique identifier in a cookie or parameter that allows the server to track requests originating from the same client. Contrast this with a traditional FTP server that conducts an interactive session with the user. During the session, a user is provided a means to be authenticated and set various variables (working directory, transfer mode), all stored on the server as part of the user's state. From Wikipedia.

STP

Spanning **T**ree **P**rotocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

Sub-ring

An Ethernet ring which is connected to one or more other Ethernet rings or networks through using a pair of interconnection nodes. On their own, the sub-ring links do not form a closed loop. A closed connection of traffic may be formed by the sub-ring links and one or more links that are controlled by another Ethernet ring or network, between interconnection nodes. From ITU-T Rec.G.8032/Y.1344 (03/2010).

Sub-ring link

A span (e.g., link/port) connecting adjacent sub-ring nodes that is under the control of the Ethernet ring protocol control process (ERP control process) of the sub-ring. From ITU-T Rec.G.8032/Y.1344 (03/2010).

Subnet Mask (Address Mask)

A bit mask used to identify which bits in an IP address correspond to the network and subnet portions of the address. Referred to as the 'subnet' mask because the network portion of the address (the network mask) can be determined by the encoding inherent in an IP address.

Synchronized clocks

Two clocks are synchronized to a specified uncertainty when they have the same epoch and their measurements of the time of a single event at an arbitrary time differ by no more than that uncertainty.

T

TACACS+

TACACS+ (**T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem **P**lus) 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.

Tag

An optional field in a frame header. In MEF 26 it is the 4-byte field that, when present in an Ethernet frame, appears immediately after the Source Address, or another tag in an Ethernet frame header and which consists of the 2-byte Tag Protocol Identification Field (TPID) which indicates S-Tag or C-Tag, and the 2-byte Tag Control Information field (TCI) which contains the 3-bit Priority Code Point, and the 12-bit VLAN ID field.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TC

Traffic Class, the new word for EXP. A 3 bit field in the 32 bit label stack entry field, which also contains 20 bits MPLS label.

TCM

Tandem Connection Monitoring (TCM) can be supported by the instantiation of a sub-path maintenance element (SPME) that has a 1:1 relationship with the monitored connection. See IETF RFC 6371 section 3.2. The SPME is then monitored using normal label switched path (LSP) monitoring. When an SPME is established between non-adjacent nodes, the edges of the SPME become adjacent at the client sub-layer network and any intermediate node that were previously in between becomes an intermediate node for the SPME. See also "SPME".

TCP

TCP (Transmission Control Protocol) is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers. The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

Telnet

TELNET (**TEL**etype **NET**work) is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client. TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

Tentative address

In IPv6, an address whose uniqueness on a link is being verified, prior to its assignment to an interface. A tentative address is not considered assigned to an interface in the usual sense. An interface discards received packets addressed to a tentative address, but accepts Neighbor Discovery packets related to Duplicate Address Detection for the tentative address.

TFTP

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) is a transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

Throttling

An S4224 function used to limit the number of multicast groups to which a switch port can belong.

ToS

ToS (**T**ype **o**f **S**ervice) is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV (**T**ype **L**ength **V**alue). An LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV. For the Type, Length, Value format, LLDP frames are sent by each equipment on each port at a fixed frequency. A frame contains a Link Layer Discovery Protocol Data Unit (LLDPDU) which is a set of type, length, value (TLV) structures. An LLDP frame should start with mandatory TLVs (e.g., Chassis ID, Port ID, and Time to live). These mandatory TLVs are followed by any number of optional TLVs. The frame should end with a special TLV named end of LLDPDU. The IEEE 802.1ab specification contains a description of all of the TLV types.

TKIP

TKIP is an acronym for **T**emporal **K**ey **I**ntegrity **P**rotocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

Transparent clock

A device that measures the time taken for a Precision Time Protocol event message to transit the device and provides this information to clocks receiving this PTP event message.

Two-step clock

A clock that provides time information using the combination of an event message and a subsequent general message.

U

UDP

UDP (**U**ser **D**atagram **P**rotocol) is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers. UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact. Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UNI

(User Network Interface) the physical interface or port that is the demarcation between the customer and the service provider/Cable Operator/Carrier/MSO per MEF 4.

UNI-C

UNI – Customer per MEF 4. A compound architectural component on the Subscriber side of the UNI that represents all the functions required to connect a subscriber to a MEN (per MEF 27).

UNI-N

UNI – Network per MEF 4. A compound functional element used to represent all of the functional elements required to connect a MEN to a MEN subscriber implementing a UNI C. The functional elements within the Customer Edge that supports the MEN Subscriber's technical capabilities and compliance to the UNI specification. A set of one or more functional elements that supports the MEN Service Provider's technical capabilities and compliance to the UNI specification. (Per MEF 27.)

Unicast address

In IPv6, an identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address.

Uniform Model

One of three different Diffserv tunneling models defined in RFC 3270, and which define e.g. inheritance of TTL and EXP/TC in the label stack during push and pop. TTL inheritance is defined in RFC 4343. See also "Pipe Model" and "Short Pipe Model".

UPnP

UPnP (**U**niversal **P**lug a**n**d **P**lay). The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components.

Upper layer

In IPv6, a protocol layer immediately above IPv6. Examples are transport protocols such as TCP and UDP, control protocols such as ICMP, routing protocols such as OSPF, and internet or lower-layer protocols being "tunneled" over (i.e., encapsulated in) IPv6 such as IPX, AppleTalk, or IPv6 itself.

Upstream-assigned label

Label used for MPLS multicast packet where the label comes from the upstream LSR label space (normally the label comes from the downstream LSR label space). RFC5332 redefines Ethertype 0x8848 (formerly the multicast MPLS Ethertype) to indicate the top label is upstream-assigned.

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

V

Valid IPv6 address

In IPv6, a preferred or deprecated address. A valid address may appear as the source or destination address of a packet, and the internet routing system is expected to deliver packets sent to a valid address to their intended recipients. See the IETF "Recommendation for IPv6 Address Text Representation" or use a validator for IPv6 address formats such as http://www.intermapper.com/ipv6validator.

Valid lifetime

In IPv6, the length of time an address remains in the valid state (i.e., the time until invalidation). The valid lifetime must be greater then or equal to the preferred lifetime. When the valid lifetime expires, the address becomes invalid.

VeriPHY®

Cable diagnostics that detect cable conditions such as cable length, opens, shorts, coupling between pairs, and termination status. 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.

VLAN

Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This 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 switch does not remove or insert VLAN tags.

VLAN aware switching: This 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.

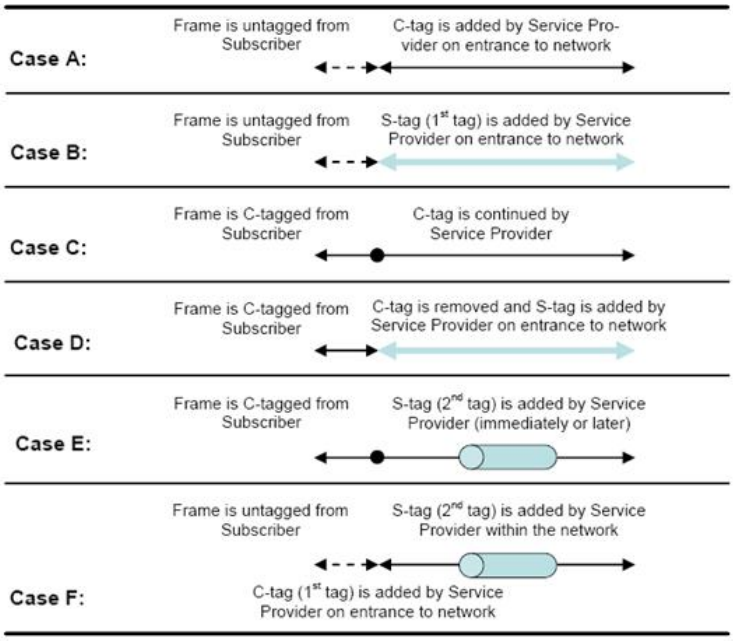
Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames 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.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

VLAN Tagging

In cases A - D below, a SOAM PDU is initiated by a Customer, and as it flows over the data path it continues to be processed and treated as a SOAM PDU. These frames exist in the OAM Flow Space seen by the Service Provider and the Operator. Thus MEG Levels used at any point can be seen by any other point in the path (subject to [IEEE 802.1ag restrictions on the extent of the MEG Levels). So different parties, such as the Service Provider and Operator, must coordinate the use of all levels that they share.



In Cases E and F above, the SOAM PDUs that were inserted in the un-tagged or single-tagged portions of the path are invisible to all points that are double tagged (since the double-tagged part of the path (the 'tunnel') has hidden the fact that a frame is a SOAM PDU with the addition of a second (outer) tag). These frames do not exist in the OAM Flow Space seen by the Service Provider and the Operator. Within the double-tagging, SOAM PDUs can be inserted and they can use any MEG Level without consideration for the MEG levels used by SOAM PDUs that use single tags.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

VoIP

Voice over Internet Protocol.

VTY

(Virtual Type Terminal) - A **vty** interface and password must be created in order to enable Telnet access to an IPv6 router. Also Virtual TTY (VTY).

W

WTB

The Wait To Block (WTB) timer is employed by the RPL owner to delay reversion after a forced switch or manual switch has been cleared. From ITU-T Rec.G.8032/Y.1344 (03/2010).

WTR

WTR (**W**ait **T**o **R**estore) is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.

Index

prompt 384
> prompt 383
1:1 port protection scheme 92
N port protection scheme 92
ACE 76
ACL 76
API Inst 380
auth 272
change password 87
CLI editing 26
CLI help 26
CLI history 26, 27
COM port seetings 9
comment lines 20
config file 19
config files, types 46
Configuration commands 71
Configuration methods 9
configure terminal 71, 167
Down MEP 175
DST 82
E-Access service 116
E-LAN 106
E-LAN service 115
E-Line 106
E-Line service 115
engine ID 271
ENNI 116
EPL service 115
EP-LAN service 115
Ethernet port 25
Ethernet Private Tree service 116
Ethernet switch ID 25
E-Tree 106
EVC types 106
EVPL service 115
exit a mode 16
filtering 30
global configuration mode 36
GVRP 118, 119
Help styles 64
Help system 120
HyperTerminal 9
IEEE 1588 232
Ingress BWP 112
keyword 22
LACP 166
LAG 166
LOAM commands 310
Management methods 9
Management VLANs 17
MEG levels 175
MEP frame loss measurement 199
MEP parameters 185
MEP PM 206, 207
MIB View 280
MIP 175
MIP parameters 204
modes 31
modes - exceptions 32
no command 58
nothing is output 43
output filtering 30
parameter 22
parent mode 31
password, admin 16
PHY 378, 379
port protection schemes 88
privelege levels 15
privilege levels 34
PTP clock modes 237
PTP parameters 232
PTP time 233
QCE 395
QCL 395
QoS parameters 248, 259, 261, 262
QoS QCE 253, 259
QoS QCL 253
Quality of Service 248, 259, 261, 262
RADIUS 264
Reset to factory defaults 15
RMON Configuration 267, 397
serial console 21
SNMP 271
SNMP Community 273
SNMP Engine 275
SNMP Host configP 275
SNMP MIB View config 280
SNMP security model 276
SNMP server version config 280
SNMP trap config 277
SNMP user config 278
SNMP v3 config 274
software image, Active 48
software image, Alternate 48
software images, swapping 48
software images, types 48
ssh 21
STP config 281
sub-mode 31
Syslog Events 172
TACACS+ 287
TAI time 233
telnet 21
terminal emulation program 9
time of day 82
ToD 82
Trap 271

trap events....131
Up MEP....175
upgrade firmware....48
Upgrade firmware....306
user accounts....39
Users, adding....39
Users, deleting....39
Users, modifying....39
UTC time....233
VLANs....16
Voe....373
Vola....373

Transition Networks

10900 Red Circle Drive

Minnetonka, MN 55343 USA

Tel: 952- 941-7600 or 1-800-526-9267

Fax: 952-941-2322

Printed in the U.S.A.

S4xxx CLI Reference 33559 Rev B